

Initial Coin Offering and Cryptocurrencies: Shifting Trust Away from Human Actors and toward a Cryptographic System

George Bouchagiar

University of Antwerp, Antwerp, Belgium
Email: georgebouchayar@yahoo.gr

How to cite this paper: Bouchagiar, G. (2018). Initial Coin Offering and Cryptocurrencies: Shifting Trust Away from Human Actors and toward a Cryptographic System. *Journal of Financial Risk Management*, 7, 386-427.

<https://doi.org/10.4236/jfrm.2018.74022>

Received: October 25, 2018

Accepted: December 4, 2018

Published: December 7, 2018

Copyright © 2018 by author and
Scientific Research Publishing Inc.

This work is licensed under the Creative
Commons Attribution International
License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

Abstract

Initial Coin Offering (ICO) has become global. Cryptocurrencies are offered to finance projects in the blockchain arena. This crypto-phenomenon challenges traditional capital raising and investment mechanisms and many strongly believe in its potential. This paper analyses some key characteristics of ICOs and investigates potential risks. It also examines the shift from traditional mechanisms to “cryptos” and studies several features of blockchains. An overview on trust is provided to detect some trust-enhancing and trust-diminishing aspects of technologies. Finally, cryptology is discussed to test cryptocurrencies’ potential as objects of trust.

Keywords

Cryptocurrencies, Initial Coin Offering, Money, Trust, Cryptology

1. Introduction

Initial Coin Offering (ICO) has become a hotly debated topic (Li & Wang, 2017: p. 49; Kristoufek, 2013: p. 5; Williamson, 2018: p. 111; Corbet, Lucey, & Yarovaya, 2018). While its true potential may become apparent only many years after it is generally adopted (Berentsen & Schär, 2018: p. 13), albeit some of its aspects could safely be addressed. This paper examines some basic features of this new crypto-phenomenon to compare it with other funding mechanisms and point out some risks emerging from ICOs. It, then, studies the shift from “traditional money” to cryptocurrencies and highlights some basic features of blockchains, the basis on which these new systems operate. An overview on the multiple facets of trust is provided to further examine trust-enhancing and trust-diminishing factors in fields of technology. Finally, cryptology, the science

behind cryptocurrencies, is discussed to test their potential to be trusted.

In 2012, the European Central Bank stated that virtual currency schemes (or *digital representation of value*; Financial Action Task Force, 2014: p. 4; European Central Bank, 2015: p. 4) did not pose a risk to price stability; the money creation continued to stay at a low level (European Central Bank, 2012: p. 47). They could not jeopardize financial stability due to their “*limited connection with the real economy, their low volume traded and a lack of wide user acceptance*” (European Central Bank, 2012: p. 47).

But this was in 2012.

Today, Initial Coin Offering, a new funding opportunity (Hartmann, Wang, & Lunesu, 2018: p. 33, 37) also known as Initial Cryptoasset Offering (ICO) or Initial Token Offering (ITO), is a global phenomenon; it is a *global ocean* (Thompson, 2018: p. 14) that has become widespread in terms of adoption, number of currencies available and market capitalization (Fenu, Marchesi, Marchesi, & Tonelli, 2018: p. 26, 27). ICO has been defined as public offers of new cryptocurrencies (i.e. a medium of exchange, created and stored in the blockchain, using encryption techniques to *control* the creation of monetary units and *verify* the transfer of funds; Roettgers, 2018: p. 44) in exchange for existing ones to finance projects in the blockchain arena (Fenu, Marchesi, Marchesi, & Tonelli, 2018; Roettgers, 2018; Gray, 2017). The token may qualify as a financial instrument (ESMA, 2017) and has been regarded as something serving as a “*visible or tangible representation of a fact*” or as a voucher that can be exchanged for goods or services, or a sign, a symbol, an evidence of the existence of an event (UK Consumer Credit Act, 1974: Section 14; Conheady, 2018; Oxford Dictionary, 2018). To some authors, it has the characteristics of a digital voucher and grants participants a right that may represent a license to use a software program (usage token), a membership in a community (community token), a financial asset (Zetzsche, Buckley, Arner, & Föhr, 2018: p. 8); it can portray a commodity, currency or collectible (Hartmann, Wang, & Lunesu, 2018: p. 33). Therefore, tokens may be understood as cryptographically-secured coupons that embody a bundle of rights or obligations (Monetary Authority of Singapore, 2017: paragraph 2).

And there may be pure but also hybrid token types. Pure types include tokens with an investment, a utility, or a currency component. In particular, investment tokens involve an expectation of profit and their holders can be understood as members of a blockchain-based investment vehicle (Hacker & Thomale, 2017: p. 25-26). Utility tokens confer rights to use products developed by the issuing firm and deposited on the blockchain (Hacker & Thomale, 2017: p. 28). And currency tokens share some characteristics with bearer instruments, such as liquidity, and can—to some extent—be directly used as a means of payment for goods external to the blockchain, partially eliminating exchange rate risks (Hacker & Thomale, 2017: p. 33). But, typically, tokens may share different components to different degrees. Hence, scholars argue for hybrid utility-investment, hybrid currency-investment, and hybrid currency-investment-utility tokens (Hacker & Tho-

male, 2017: p. 33-37).

In the following chapter, some further analysis is conducted to better understand ICOs' function, but also detect some risks that they may pose.

2. ICOs: Basic Properties and Potential Risks

ICO can be understood as a generalized term for using digital tokens to raise capital for a venture (Telpner & Ahmadifar, 2017: p. 16-18). Simply put, it is an *open call* for funding to raise money through cryptocurrencies (an “[...] *open call, through the Internet, for the provision of cryptocurrencies in exchange for tokens generated through smart contracts and relying on the blockchain technology, allowing the pledger to enjoy an exclusive right or reward or financial claim* [...]”; Adhami, Giudici, & Martinazzi, 2018: p. 5). This could be similar to a crowdfunding campaign, where fiat currency may be collected (Adhami, Giudici, & Martinazzi, 2018).

In particular, crowdfunding, coming from the broader notion of crowdsourcing (Belleflamme, Lambert, & Schwienbacher, 2014: p. 588; Kleemann, Voß, & Rieder, 2008), enables entrepreneurs to develop their business gradually or scale up their operations through share placement to attract venture capital funds at the early stage (Lam & Law, 2016: p. 12). In a similar way as ICO, it has been described as an *open call*. In case of crowdfunding, this open call is, essentially through the Internet, for the provision of financial resources either in the form of donation or in exchange for reward or rights to support initiatives for particular purposes (Schwienbacher & Larralde, 2012: p. 369-371). In return for their contributions, crowd funders receive either non-financial benefits or financial compensation; the rewards for investors can be social return, products or services, financial return, or refund (Buysere, Gajda, Kleverlaan, & Marom, 2012: p. 10-13). Some authors have pointed out the potential for crowdfunders to fund scams. The risk of fraud increases since the pool of funders has no personal contact or knowledge of the business idea beyond what may be presented on the relevant website (Buysere, Gajda, Kleverlaan, & Marom, 2012: p. 15). There are also technological risks that refer to problems arising with the uncertainty surrounding the determinants of performance, cost, safe operating latitudes, or failure modes. Such risks play an important role in the funder's decision to invest (Bento, Gianfrate, & Groppo, 2018: p. 2).

Compared to crowdfunding, ICO can offer buyers of digital tokens the right to use them at some future date to, e.g., buy a product or service that the firm will develop (Michaels, 2017). It seems that both ICO and crowdfunding ask for an *all-or-nothing* contribution to start the project setting a minimum contribution price. And they both enable to test the demand for the product or service; they may allow adapting production to market demand (Cerezo Sánchez, 2017: p. 3).

In some cases, ICO may involve securities (Paech, 2011; Securities and Exchange Commission, 2017a), but, as authors have argued, it should be decided

on a case-by-case basis whether the tokens are designed in a way that makes securities regulation applicable or not (Hacker & Thomale, 2017: p. 20, 39). In its guidelines (February 16, 2018), the Swiss Financial Market Supervisory Authority (FINMA, 2018: p. 3-6) distinguished between payment tokens, utility tokens, and asset tokens. To FINMA, payment tokens are intended to be used as a means of payment for acquiring goods or services or as a means of money or value transfer. Since these tokens are designed to perform as a means of payment, they are not analogous to traditional securities. Utility tokens are intended to provide access to an application or service by means of a blockchain-based infrastructure. If these tokens aim just to confer access to a service or application and if they can actually be used this way at the point of issue, FINMA will not treat them as securities. But if a utility token has an investment purpose at the point of issue, it will be treated as a security. Finally, asset tokens represent assets, like a debt or equity claim on the issuer, and the Swiss Financial Market Supervisory Authority treats them as securities, when they represent an uncertificated security and they are standardized and suitable for mass standardized trading.

Moreover, the Gibraltar Financial Services Commission (GFSC, 2017) has stated that tokens may represent securities, e.g. shares in a company, and, thus, their promotion and sale may be regulated as such. Yet more often they serve some cryptocurrency or functional use that is not regulated, e.g. prepayment for access to a product or service that is to be developed using funds raised in the ICO. Hence, as the HM Government of Gibraltar (Gibraltar Finance, 2018) has mentioned, unless structured as a security or as a debt instrument, tokens do not constitute any form of regulated financial instrument in the European Union; they and their sale are unregulated.

Interestingly, in case *Skatteverket v. David Hedqvist*, the CJEU found that Bitcoin, being a contractual means of payment, cannot be regarded as a current account or a deposit account, a payment or a transfer; unlike a debt, cheques, and other negotiable instruments, the Bitcoin virtual currency is a direct means of payment between the operators that accept it (CJEU, 2015: paragraph 42). To the CJEU, it is common ground that the Bitcoin virtual currency is neither a security, conferring a property right, nor a security of a comparable nature (CJEU, 2015: paragraph 55). But it should be noted that this decision concerned the VAT treatment of Bitcoins, not securities regulation.

In the United States, in case of “The DAO”, a Decentralized Autonomous Organization that aimed to sell tokens to investors through an ICO, the U.S. Securities and Exchange Commission (SEC) found that these tokens qualified as securities under the U.S. securities laws. The SEC accepted that securities include an investment contract, which is an investment of money in a common enterprise with a reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others (Securities and Exchange Commission, 2017a). Yet the SEC did not hold that all ICOs involve securities. Joseph Grund-

fest, who used to be a commissioner at the SEC in the 1980s, stated that ICOs represent the most pervasive, open, and notorious violation of federal securities laws since the Code of Hammurabi (Popper, 2017).

So, it can be clear that, at least in a number of cases, ICOs are not regulated.

In contrast to traditional capital raising or investment mechanisms, the decentralized nature, in conjunction with the above lack of laws and regulation (Conley, 2017)¹ in the blockchain environment (Veuger, 2018)², offers flexibility to both investors and startups (Abgaryan, Liu, Menteshashvili, Abgaryan, & Gao, 2017). In particular, there can be multiple features that distinguish ICO from other mechanisms. Namely, no fiat currency can be *directly* applied, since one has to use, e.g., Bitcoin or other cryptocurrencies to participate in ICOs (Abgaryan, Liu, Menteshashvili, Abgaryan, & Gao, 2017: p. 2). But purchasers may be able to use fiat currency, like U.S. dollars, to buy virtual coins or tokens (Securities and Exchange Commission, 2017a: 6; 2017b; Pangas & Park, 2017: p. 16). Moreover, in ICO, there are no regulatory limitations set on the qualification of investors or factors as regards startups (Abgaryan, Liu, Menteshashvili, Abgaryan, & Gao, 2017: p. 2). However, there could be other kinds of limitations; for instance, the entrepreneur may have limited pricing power, e.g. after the token sale, since the price might fluctuate (Cerezo Sánchez, 2017: p. 3). Furthermore, ICO issuers can be entity based (centralized) or non-entity based (decentralized) (Abgaryan, Liu, Menteshashvili, Abgaryan, & Gao, 2017: p. 2); and, in the absence of intermediaries, such as banks, funds could be directly distributed.

But ICO may involve risks. Investors may feel defrauded or wronged when the investment is unsuccessful (Carlson & Selin, 2018: p. 18). In its press release (September 25, 2017), the U.S. Securities and Exchange Commission called out a focus on violations involving distributed ledger technology and initial coin offerings (Securities and Exchange Commission, 2017c). In fact, trading tokens is susceptible to price manipulation and other fraudulent trading practices (Clayton, 2017). Associations, such as the North American Securities Administrators Association (NASAA, 2018), warn that concerns, which investors should consider before investing in any offering, may include: the fact that cryptocurrencies are subject to minimal regulatory oversight and susceptible to breaches and hacks; the high volatility of such investments may make them unsuitable for most investors and, in particular, for those who would wish to invest for long term goals; investors could be highly reliant upon unregulated firms, which might lack internal controls or may be susceptible to fraud and theft; and investors may have to rely upon the strength of their own computer security systems, but also security systems provided by third parties, to protect purchased crypto-

¹As Conley (2017: p. 2) argues, if crypto-tokens are currency they need to comply with the know your customer and the anti-money-laundry regulations; if they are a form of stock or security, start-ups must comply with the relevant rules and regulations for the securities and exchange.

²Blockchain is stated to be a combination of cryptography (a digital token with monetary value) and a shared distributed ledger with synchronized data spread across multiple sites, countries and institutions (Veuger, 2018: p. 108). To Veuger, blockchain, like money, can be spent once (Veuger, 2018: p. 112).

currencies from theft.

And fraud has been perpetrated in a number of cases. In 2017, the U.S. Securities and Exchange Commission obtained an emergency asset freeze to halt a fast moving ICO fraud that raised up to 15 million U.S. dollars from many investors by falsely promising a 13-fold profit in less than a month (Securities and Exchange Commission, 2017d). In another case, in its “Emergency Cease and Desist Order”, the Texas State Securities Board, treating the investments in the BitConnect Staking Program and the BitConnect Lending Program as securities, found that the firm had engaged in fraud in connection with the offer for sale of securities and had made statements materially misleading, or otherwise likely to deceive the public (Texas State Securities Board, 2018: p. 8-9). And, interestingly, in 2017 China banned ICOs outright (Ruwitch & Kelly, 2017).

With all the above features and risks involved, ICOs, a vehicle to raise early capital (Conley, 2017), may include a business idea, which is often described in a white paper (Adhami, Giudici, & Martinazzi, 2018: p. 3), a proposer team, a target sum to be collected, a given number of tokens, of new cryptocurrency to be given to subscribers according to a predetermined exchange rate with one or more existing cryptocurrencies (Fenu, Marchesi, Marchesi, & Tonelli, 2018: p. 26, 27).

To gain some insight into the basis on which these new mechanisms operate, the shift from “traditional money” to cryptocurrencies is studied below.

3. From Cash to Crypto

On the 27th of February 1797, people who went to the Bank of England found a handbill stating that the Council had ordered the Bank’s directors to forebear issuing any cash in payment (Chadha & Newby, 2013; Acres, 1931; Newby, 2007). While one could previously demand exchanging a banknote into coins (Shin, 2015)³, this was no longer the case; the banknote became a “*promise to pay promises with promises*” (Barry, 2007: p. 55).

While some have argued that it is not easy to define “money”, others believe that it can be defined by its functions (Reuten, 1988: p. 121). Being a “*creature of the law*” (Knapp, 1924: p. 1), it may be understood as a numeraire, a medium of exchange, a store of value, a means of payment, a unit of account, a measure of wealth, a simple debt, a delayed form of reciprocal altruism, a reference point in accumulation, an institution, or a combination of the above (Bell, 2001: p. 150). Money may also function as a liquid asset, a framework of the market allocative system, or a controller of the economy (Davies, 2002: p. 27-28). It may act as the

³In most of its history, money has been identified with precious metals, mainly gold or silver; the introduction of paper money in Europe in the 17th century maintained the link *via* convertibility (Shin, 2015: p. 417). In accordance with the *metalist idea* of money, its foundation was found in the value of scarce metals (Appleby, 1976). This was challenged by inconvertible paper money, like the French assignat (Chown, 2003: p. 37). In accordance with the *nominalist view*, money does not have to consist of metal; paper could also be a legitimate form (Sargent & Velde, 1999). The debates between nominalists and metalists have been regarded as battles over the *metaphysics of money* (Shin, 2015: p. 418, 434).

material, in which the magnitudes of value of commodities are expressed socially (Rosdolsky, 1977: p. 137). Furthermore, it is accepted that money is credit –the correlative of debt– representing a debt relation, a promise or an obligation that exists between human beings; to some, it cannot be identified independently of its usage (Bell, 2001). Money can be regarded as socially constructed, shaped by social relations, as something that also exists outside of the market and that is profoundly influenced by cultural and social structures (Nyman, 2003: p. 79). In this context, values and social relations reciprocally transmute—different kinds of—money (Nyman, 2003: p. 79) by investing it with meaning and social positions (Knapp, 1924: p. 93-111). Being understood as a *réalité sociale* (Simiand, 1934; Zelizer, 1989: p. 343) that transformed the world into an arithmetic problem (Simmel, 1950: p. 412) and brought an objectification or a *factification* of value (Lash, 2007: p. 64), money is often a central point of theories that aim to improve societies (Blanc, 1998: p. 469). It has been viewed as a necessary medium of exchange, and, to some, its organization is transformed to suppress the disastrous effects of speculation, hoarding, or usury, that are considered to be sources of economic crisis (Blanc, 1998: p. 470). Since one of the main functions of money is in its circulation, it has been regarded as a *perpetuum mobile* that must have a means of circulation (Herland, 1977).

With cash⁴, money becomes a concrete reality in people’s hands (Abramovitch, Freedman, & Pliner, 1991: p. 29; Desan, 2014). Maybe, cash has not yet become history, but it would be fair to argue that, in several jurisdictions, it is used less than ever before (Swift & Ander, 2016; Federal Reserve Board, 2016); and it cannot be used at all to make payments in some places, like for in-flight purchases on airplanes (Angel & McCabe, 2015: 605).

Cash is held, because it can be given up at the appropriate time (Baumol, 1952: p. 545). It solves the problem of double spending by virtue of its materiality. One cannot give cash away twice to two different parties (Maurer, Nelms, & Swartz, 2013: p. 264). To some authors, payment by cash is the most transparent form of payment, involving a physical price rehearsal (Kamleitner & Erki, 2013: p. 58). But risks could occur, since cash can be transferred physically and it may be difficult to ascertain its source and impossible to know the intended beneficiary (Europol, 2015: p. 9). When cash, as a physical object, is transferred, its value is transferred as well. There is no need for a third party to intervene or for a central authority to keep accounts (Berentsen & Schär, 2018: p. 1-2). The par-

⁴Under Article 2(2) of the Regulation (EC) No 1889/2005 of the European Parliament and of the Council of 26 October 2005 on controls of cash entering or leaving the Community, “cash” means: (a) bearer-negotiable instruments including monetary instruments in bearer form such as travelers cheques, negotiable instruments (including cheques, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery and incomplete instruments (including cheques, promissory notes and money orders) signed, but with the payee’s name omitted; (b) currency (banknotes and coins that are in circulation as a medium of exchange).

⁵The *perfect* anonymity, an appealing characteristic of paper money, was strongly advocated to grant privacy in e-money systems; but it had its dark side, since it enabled *perfect* crimes (Jakobsson & Yung, 1997: p. 218).

ties may remain anonymous⁵, camouflaged by the physical anonymity of cash (Zelizer, 1989); the one who holds it is its owner (Nyman, 2003: p. 91). Moreover, anyone can participate in the cash-system and no permission has to be obtained to gain access to cash.

But the parties involved in a transaction must be present to trade.

So, people can use letters of credit, whose basic distinction from cash security deposit is the very location of the money (Stein, 2009: p. 305). These transactions allow distant buyers and sellers to circumvent obstacles that would otherwise frustrate long-distance transactions (Gillette, 2000: p. 2537); credit, a second species of money, is built on confidence, the soul of commerce (Pagden, 1988: p. 130). Namely, the one party is confident that her money is safe and the other party is confident that he will be paid back (Jacobsen, 2010: p. 1654). This mechanism has been understood as issuing money in a form of a promise to pay cash on demand (a reason why banks may, or have, become vulnerable to bank runs; Radojičić & Radovanović, 2015: p. 376). In capitalist production, credit arises from the formation of gaps between income and expenditure and of reserve funds of money in the circulation process of capital (Reuten, 1988: p. 133). By redistributing surplus holdings of cash and by centralizing reserve holdings, the credit system can reduce the quantity of capital held in the form of money (Reuten, 1988: p. 133). In this context, the banking system has the ability to convert credit into means of exchange, payments, and circulation; the very instruments of credit may, thus, function as money (Lucarelli, 2010: p. 203).

One may deliver a letter of credit as a way to give another party comfort that she will perform her obligations (Stein, 2009: p. 299). As regards the basic structure of bank letter of credit transactions, the customer of the bank has an underlying obligation owed to a third party and that obligation is to be supported by the letter of credit. The underlying obligation may be of any type or maturity (Ryan, 1983: p. 405). Simply put, there is an import side (buyer/applicant) and an export side (seller/beneficiary); the bank of the import side can issue the letter of credit; this obligates the bank to pay upon the receipt of specified documents, e.g. an invoice or an insurance certificate (Mann, 2000: p. 2498-2499).

Therefore, the key benefit seems to be a right of payment that is enforceable against the issuer (Mann, 2000: p. 2519). Yet some have questioned the classic explanation of the letter of credit, i.e. the assurance of payment from a financially responsible third party. For example, the seller may obtain a letter of credit from a bank. But she has a right to payment, when the goods are shipped, conditioned on her presentation to the bank of the relevant documents (Özkan, Özçelik, & Kılıç, 2016; Nathan, 2003). This means that the seller's possession of an absolute right to payment could be questioned, since she may fail to provide the documents required (Mann, 2000: p. 2495; Huggins, 2012: p. 312; Barron, 2012: p. 52). From this perspective, a letter of credit could be understood, not as a means for assuring payment but, as a device to verify the reliability of the applicant/buyer or an instrument to signal the seller that the risk of the buyer's de-

fault is acceptably low (Corré, 2000: p. 2552). As some have aptly put it, firms buy letters of credit “*by mistake –because they always have*”; if they fully understood the costs, they would use alternative systems (Mann, 2000: p. 2515-2516). Other authors wonder why buyers and sellers transact through a third party that charges a significant fee for its services and is authorized to make payment notwithstanding noncompliance with the very prerequisites that it has been engaged to monitor (Gillette, 2000: p. 2537). To Mann, the real function of the letter of credit is to solve information asymmetries with regard to the parties involved, allowing the issuer with superior information to verify a buyer’s legitimacy to the distant seller (Mann, 2000).

In addition to the letters of credit, another way to generate distant transactions is electronic payment. E-money has been defined as electronically stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions and which is accepted by a natural or legal person other than the electronic money issuer (Halpin & Moore, 2009: p. 565). E-payment allows transmission of value by electronic means, decreasing costs of physical transmission (Morse, 2018: p. 946-948; Grüşchow, Kemper, & Brettel, 2016). However, as regards the above mechanisms—both electronic payment and letters of credit—the parties need an intermediary; a person to trust; one to act as a guardian; one who will not run away with the money (Berentsen & Schär, 2018: p. 3). Therefore, people who may not trust each other can trade because they both can trust the intermediary.

But some state that new technologies, i.e. blockchains and their alleged features, e.g. public accessibility, immutability or resilience (Xu, Shah, Chen, Diallo, Gao, Lu, et al., 2017: p. 16), can mathematically provide trust in a network that is the very trusted party, overseeing and auditing the proper completion of transactions (Nakamoto, 2008). Experts promise that people will enjoy trustworthiness in systems, where each element, being fully dynamic and not tied to specific physical space, will not be managed as a physical object (Buterin, 2014).

Blockchain has been described as a chain or string of blocks. Each block is composed of a part representing a fact, like a transaction, and a part (the header) containing information, e.g. timestamp or hash, and the hash of the previous block (Hammi, Hammi, Bellot, & Serhrouchni, 2018: p. 127). It has been understood as a technology designed to maintain continuity—meaning the blocks follow one another in a sequence—and reliability—meaning the impossibility of replacing or removing a link from the chain (Biktimirov, Domashev, Cherka-shin, & Shcherbakov, 2017: p. 235). Blockchain has also been regarded as a decentralized chain that relies on a peer-to-peer network, where each node maintains a copy of the ledger to prevent a single point of failure; all copies are said to be updated and validated simultaneously (Hammi, Hammi, Bellot, & Serhrouchni, 2018: p. 127). These technologies are said to differ from existing networks as regards how transactions occur and how information can be stored and secured (Funk, Riddell, Ankel, & Cabrera, 2018: p. 3-4). They have been referred to as distributed transaction databases, in which different nodes cooperate as a

system to store sequences of bits that are encrypted as a single unit or block and then chained together. As authors argue, blockchains involve a cryptographically secured distributed ledger with a decentralized consensus mechanism (Risius & Spohrer, 2017; Shiho, 2018; Levin, 2014). In this context, an “object”, e.g. a right, may be tokenized and registered in the blockchain. So, its subsequent disposal may be performed by means of disposal of its digital *alter-ego* (Savelyev, 2018: p. 864). The process of hashing transforms tangible—e.g. raw material—or intangible ownership of a file-asset into digitally encoded tokens (Francisco & Swanson, 2018).

Focusing on cryptocurrencies, Lemieux (2016: p. 119) provides an apt, yet technical, overview of the process concerning Bitcoin blockchain: X proposes the transfer of Bitcoin to Y; the network checks that there is sufficient Bitcoin in X’s wallet; nodes—or miners—(Williamson, 2018: p. 107) bundle the proposal with other transactions to create a new block; the blocks, as time stamped batches of valid transactions (Ølnes, Ubacht, & Janssen, 2017: p. 356), are cryptographically hashed (i.e. they are used as input to an algorithm that converts them into an alphanumeric string, the hash value); the hash is put into the header of the proposed block; the header becomes the basis for the proof of work (Buterin, 2013) performed by the nodes on the network; when a node reaches a solution to the proof-of-work, other nodes check it and then each; the node that confirms the solution updates the blockchain with the hash of the header (of the proposed block); this becomes the new block’s identifying string (and is part of the distributed ledger); the transaction is confirmed.

X pays Y.

Simply put, blockchain is a software solution protocol and can be understood as children playing basketball: the game is successfully played in the absence of a referee, as all kids are aware of the rules and play according to them; all agree on the score, so, there is no need for a score keeper; in case of a foul, children reach consensus and continue playing; no kid can change the rules, but any child may leave or join as long as she accepts the score and the rules (Burger, Kuhlmann, Richard, & Jens Weinmann, 2016; Buterin, 2014; Funk, Riddell, Ankel, & Cabrera, 2018; Hoy, 2017; Iansiti & Lakhani, 2017; Rethink Music, 2015).

In essence, blockchain can act as a secure architecture, as a ledger to handle and store events, e.g. transactions (Lemmen, Vos, & Beentjes, 2017: p. 491). It is possible that anyone can hold a copy and read or write to it. One could argue that this could lead to fraud as anyone would simply create or remove facts. However, this can be practically prevented by cryptography. The latter makes it difficult to change events and can, thus, assure that what is in the ledger is genuine. Each block has information about the previous block that is, then, cryptographically hashed with data about the relevant transaction (Mansfield-Devine, 2017: p. 15); so, the authenticity of each item of information can be verified by the ones that preceded it. Furthermore, since blockchains can be shared among users, they may be open to scrutiny (Mansfield-Devine, 2017: p. 15). In this context, contracts could be embedded in digital code and stored in

transparent databases. They could be protected from deletion or tampering. Any task could have a cryptographic signature that would be identifiable; it could be validated. This might affect any intermediary, from lawyers and notaries to bankers. Some argue that this capacity to freely transact and interact could change the world as we know it. This is regarded as the immense potential of blockchains (Iansiti & Lakhani, 2017).

Therefore, firms and organizations (Perez, 2015) are looking to use this sophisticated and distributed online ledger (Ølnes, Ubacht, & Janssen, 2017: p. 355; Zyskind, Nathan, & Pentland, 2015) for several reasons (Webb, 2015; Yli-Huumo, Ko, Choi, Park, & Smolander, 2016: p. 2; Lachance, 2016; Orcutt, 2015; Xu, Xu, & Li, 2018; Kshetri, 2017: p. 1030; Conti & Kumar, 2017; World Economic Forum, 2016). Since blockchain is said to allow people, who have no confidence in each other, to collaborate without having to go through a neutral central authority (Otte, Vos, & Pouwelse, 2017), it is argued that it could function as a machine for *creating trust* (Economist, 2015) or as a shared, trusted and public ledger that anyone could inspect but that no single user would control (Shackelford & Myers, 2017; Findlay, 2017: p. 179).

And blockchains seem to aim at a community mechanism (Meyer & Hudon, 2018: p. 10), which might be in contrast with traditional hierarchical mechanisms⁶ of money (Bell, 2001: p. 149; Mehrling, 2013; Peters, Panayi, & Chapelle, 2015; Adler, 2001). Money has been regarded as a symbolic token (Bachmann & Kroeger, 2017: p. 12) that needs trust⁷ to work (Beckert, 2006; Desmet, Cremer, & Dijk, 2011). As some have put it, all money is fiduciary or trust⁸ (Reuten, 1988: 137; Conley, 2017: p. 3). Thus, discussing trust would be needed to examine cryptocurrencies' potential to be trusted.

4. The Multiple Facets of Trust

Trust tends to be like a combination of the weather and motherhood; it may be widely talked about and widely assumed to be good; but when it comes to specifying just what it means vagueness creeps in (Porter, Lawler, & Hackman, 1974: p. 497). To some, the *locus of trust* is likely to be diverse in any given situation (Davenport, Dibben, Friedman, Marsh, Rosenbaum, & Thimbleby, 2000: p. 239);

⁶Always and everywhere, monetary systems are hierarchical (Mehrling, 2013: p. 394). Some mention several differences between centralized virtual currencies and crypto-currencies: in terms of changes to their specification (in crypto-currencies the specification is agreed by cryptographic consensus); in terms of purpose and geographic area of operation (crypto-currencies aim at use in the wider economy); in terms of the existence (in crypto-currencies there is no centralized authority and transactions are generally irreversible); in terms of flow of currency between users and the currencies' exchangeability with fiat; and in terms of the value generation mechanism (Peters, Panayi, & Chapelle, 2015). Adler (2001: p. 218) suggests that there are three ideal-typical governance mechanisms: market/price (that operates on grounds of prices), hierarchy/authority (where the authority connects expectations and interactions), and community/trust (that requires trust as a mechanism to control communication between actors).

⁷To others, money works best when it can be taken for granted and its social construction is hidden (Carruthers & Babb, 1996: p. 1556).

⁸Zelizer (1989: p. 359), citing Dorothy Dix, remarks on the irony of a man, who "*will trust a wife with his honor, his health, his name, his children, but he will not trust her with money*".

it is a multifaceted concept (Mishra, 1996) that is difficult to define (Lanford, 2006); it needs a specific context (Lewicki & Bunker, 1995).

Trust (Frankel, 1983) has been understood as a particular level of the subjective probability (Rempel, Holmes, & Zanna, 1985: p. 96) with which an agent assesses that another agent or group of agents will perform a particular action both before she can monitor this action and in a context in which it affects her own action (Gambetta, 1988: p. 217). To some, trust has an ethical facet; it may be the result of right, just, and fair behavior—meaning morally correct decisions and actions based upon the ethical principles of analysis—that recognizes and protects the rights and interests of others within a society; it is the expectation of ethically justifiable behavior (Hosmer, 1995: p. 399). To others, the issue is not moral; trust has strategic and calculative dimensions, it is office politics (Burt & Knez, 1996: p. 70). But most agree that trust is a psychological state “*comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another*” (Rousseau, Sitkin, Burt, & Camerer, 1998: p. 394-395; Leib, 2007: p. 643). It is an internal state of the trustor with cognitive and affective components, rather than an observable behavior (McKnight & Chervany, 2000). Being this willingness to accept vulnerability, trust is an essential element of any activity, in which people are involved (Leib, 2009: p. 693; Baier, 1994: p. 133).

As some have put it, trust begins where prediction ends (Lewis & Weigert, 1985: 976). It must go beyond predictability (Deutsch, 1958). Another party's predictability is not sufficient to make a person willing to take a risk. As Mayer, Davis, and Schoorman have aptly put it, if one's superior always shoots the messenger when bad news is delivered, the superior is predictable; but this predictability will not increase the likelihood that the individual will take a risk and deliver bad news (Mayer, Davis, & Schoorman, 1995: p. 714).

Honesty is also involved, since trust in some degree of veracity functions as a foundation of relations among human beings (Bok, 1978: p. 31). Being the mutual *faithfulness* on which all social relationships ultimately depend, trust deals with truth telling and keeping promises (Post, 2011: p. 1165-1166). From a sociological perspective, trust is a property of collective units, not of isolated individuals (Lewis & Weigert, 1985: p. 968). Yet, to others, trust is personal, relative, situational, and fluid; it highlights everything we have accomplished as human species (Schneier, 2015: p. 212).

Trust has also been defined as the very condition of the possibility of the existence of differentiated socio-economic systems (Giddens, 1990; Luhmann, 1979; 1995). It is a blending of knowledge and ignorance (Simmel, 1950: p. 318; Braun, 2016: p. 1070), which is needed to perform as a *sense making process* (Arnoldi, 2010: p. 31) to reduce the complexity of contemporary societies (Lewis & Weigert, 1985: p. 968). It is something not static (Koza & Lewin, 1998) and, to some, an undertheorized, an under-researched, and a poorly understood phenomenon (Child, 2001: p. 275). While it is central in people's lives, scholars rarely discuss it; they only treat it as a background environment (Dasgupta, 1988: p. 49); it is

not a topic of “mainstream” literature (Luhmann, 1988: p. 94).

A necessary condition of trust is interdependence, where the interests of one party cannot be achieved without reliance upon another (Rousseau, Sitkin, Burt, & Camerer, 1998: p. 395). So, trust involves risk and doubt (Lewis & Weigert, 1985: p. 968), reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values (Mayer, Davis, & Schoorman, 1995: p. 712; March & Shapira, 1987: p. 1404; Currall & Judge, 1995). In this context, it has been described as the decision to rely on another party under a condition of risk or a condition of the subjective possibility of loss, as perceived by the decision maker (Chiles & McMackin, 1996: p. 90; Currall & Inkpen, 2006: p. 236). As authors have argued, risk creates an opportunity for trust that leads to risk taking (Rousseau, Sitkin, Burt, & Camerer, 1998: p. 395; Egger, 2001); it is a characteristic of decisions that is defined as the extent to which there is uncertainty about whether potentially significant and/or disappointing outcomes of decisions will be realized (Sitkin & Pablo, 1992: p. 10). Risk can, thus, be understood synonymously with uncertainty (Grabner-Kräuter & Kaluscha, 2003); it can be the probability of an adverse future event multiplied by its magnitude (Adams, 2002: p. 69).

Involving the above features, trust could be regarded as the key element of healthy relationships and societies enabling an individual to be willing to make herself vulnerable to another party, to rely on another, despite potential risks that the latter will act in a way that can harm the former (Fukuyama, 1995). People are interested in trust, because it is an important lubricant of social relations and a major component of social capital, meaning features of social life, network, or norms that enable participants to act together more effectively to pursue shared objectives (Alesina & Ferrara, 2002: p. 211). Trust could, thus, be understood as the core constituent of social *cement* (Weinstock, 1999: p. 307); without trust, the everyday social life, which people take for granted, would not be possible (Good, 1988: p. 32).

In commercial relationships, trust begins with the promise that leads to a contract (Bukspan, 2013: p. 382-383). In personal relationships, the quality of a friendship depends on the extent of trust between people (Altman, 1973). Another fundamental function of trust is securing successful interactions (Alesina & Ferrara, 2002: p. 207); when people trust each other, transaction costs in economic activities are reduced, organizations function better, governments are more efficient, and financial development is faster (Uzzi, 1997: p. 37, 43, 44; Tyler & Degoey, 1996). Trust enables spontaneous sociability (Fukuyama, 1995: p. 27) that enhances well-being, altruistic behavior and the achievement of collective goals (PEW Research Center, 1997); it is, therefore, paramount for product acceptance, good working atmosphere, smooth relationships, investment criteria, and so forth (Uslaner, 2002; García-Marzá, 2005: p. 209). Without it, business is impossible and marketing fails (Audi, 2008: p. 97, 100). So, more trust may spur economic success (Glaeser, Laibson, Scheinkman, & Soutter, 2000: p. 811). It is indispensable for the effective functioning of the *symbolic media of*

exchange, like money or political power (Lewis & Weigert, 1985: p. 974). Trust can, amongst others, reduce imperfections (Qian, Zhang, & Cao, 2018), facilitate transactions (Alesina & Ferrara, 2002), promote international trade (Guiso, Sapienza, & Zingales, 2009), economic growth (Zak & Knack, 2001), micro-corporate financing (Bottazzi, Rin, & Hellmann, 2016) or mergers and acquisitions (Ahern, Daminelli, & Fracassi, 2015).

Maybe, this is the reason why trust has been understood as a valuable commodity (Casson, 1991: p. 11-12). But it is not a commodity that can be easily bought; “*if you have to buy it, you already have some doubts about what you have bought*” (Arrow, 1974: p. 23).

So, we need trust; it is the basis on which people cooperate (Blau, 1964). Its presence or absence has an important bearing on what people choose to do or even what they can do (Dasgupta, 1988: p. 51). And it is not just a modality of human actions, but also a human passion, a chosen policy for handling the freedom of other human agents or agencies (Dunn, 1988: p. 73).

Coming back to money, the latter functions best when people strongly trust in it and it cannot function at all without trust (Lewis & Weigert, 1985); people tend to trust money most when it circulates reasonably freely and naturally without manipulation⁹.

At this point, studying some factors that could enhance—or diminish—trust would be worthwhile to draw some safe conclusions as regards—the alleged *trustless*—blockchains.

5. Trust-Enhancing (and Trust-Diminishing) Aspects of Technology

As authors have found, trust improves when one party exhibits behaviors in accordance to another’s expectations (Aljukhadar, Senecal, & Ouellette, 2010: p. 105). In fields of technology, factors that may contribute to the attribution of trust could include—amongst others—competence, credibility, predictability, consistency, honesty, fairness, benevolence, loyalty, familiarity, experience, reputation, or explanation (Butler, 1991; Pettit, 1995: p. 203; Mcallister, 1995: p. 26).

Competence includes ability, capability and good judgment (McKnight, Choudhury, & Kacmar, 2002: p. 338). It may refer to one’s perception of whether an agent or a system is capable of performing the activities for which it is responsible (Butter, Liu, & Tan, 2012: p. 270). It has also been understood as the belief that the trusted agent has adequate expertise and implements the necessary techniques to ensure transaction security or to do what another party needs (Aljukhadar, Senecal, & Ouellette, 2010: p. 105; McKnight, Choudhury, & Kacmar, 2002: p. 337). In this context, it has been argued that *trust in machines* may be based mostly on the user’s perceptions of the expertise of the machine, meaning the extent to which the automation properly performs its function (Muir & Moray, 1996).

⁹To Lewis & Weigert (1985: p. 979), manipulating a monetary system is an attempt to transform a core social institution into just another commodity, like corn.

Similarly, credibility could be based on the extent to which one believes that the machine has the expertise to effectively and reliably perform the task (Ganesan, 1994: p. 3). Simply put, credibility is believability; credible agents or information are believable agents or information (Fogg & Tseng, 1999: p. 80). To some, credibility is always perceived and it includes trustworthiness and expertise—knowledge and skill (Fogg & Tseng, 1999: p. 80). In this context, a highly credible system is perceived to have high levels of trustworthiness and expertise. Besides, it is the trustor's lack of expertise—or knowledge—that makes him vulnerable and exposes him in some way (Corritore, Kracher, & Wiedenbeck, 2003: p. 742).

Predictability could be regarded as the expectation that future transactions will be successfully completed, that information will continue to be of high quality. It could be understood as one's expectations that the system will act—based on past experience—with consistency (Fogg, Marshall, Kameda, Solomon, Rangnekar, Boyd, et al., 2001; Dutton & Shepherd, 2006: p. 437, 447). And consistency may also reflect ease of use (Corritore, Kracher, & Wiedenbeck, 2003: p. 750).

Honesty is strongly related to integrity (Gefen & Straub, 2004: p. 409), sincerity, promise keeping, or not lying (McKnight, Choudhury, & Kacmar, 2002: p. 337, 339). It can be characterized by well-intentioned, truthful and unbiased actions of a system (Corritore, Kracher, & Wiedenbeck, 2003: p. 750). Honesty may be synonymous with trustworthiness, which is a characteristic of the object of trust (Corritore, Kracher, & Wiedenbeck, 2003: p. 741).

Fairness may refer to sameness, deservedness or need (Dobrin, 2012): sameness can be understood as a situation where everything is equal, no one has more than another; deservedness may refer to a notion under which one gets what she deserves, e.g. if she works hard, she succeeds and keeps all that she earns; and need could mean that those who have more to give should offer a greater percentage of what they have to help others, who are not able to contribute much (Dobrin, 2012). To some, fairness is a battle between equality and equity (Boyd, 2014). In this context, it could be met, if the system treated everyone equally or equitably based on their performance and needs (Leventhal, 1980). Authors have also argued that people's perceptions of fairness could be their "*beliefs in a just world*" (You, 2012: p. 703).

Benevolence goes beyond fairness (Deutsch, 1958). It demonstrates concern for the well-being of others (Tian & Sanchez, 2017: p. 235-236). It refers to actual care or goodwill and it is based on perceived motives (Gefen & Straub, 2004: p. 409). Benevolence represents kindness and altruism that reduce concerns about uncertainty or opportunism; it, thus, includes not acting opportunistically or manipulatively (McKnight, Choudhury, & Kacmar, 2002: p. 338). It could refer to one's perceptions of an agent's efforts and "willingness" to achieve some value that is desirable, without seeking rewards (Wu, Huang, & Hsu, 2014: p. 191, 196). But there could also be cases, where the trusted agent would "wish" to maintain a mutually rewarding relationship with the trustor, while the trustor would wish stability and durable policies. And this mutuality could also enhance trust (Six & Sorge, 2008: p. 859, 860). It could give some perception of ability to

ensure the trusted agent's commitments to act in the interest of the trustor (Bauer & Fatke, 2014: p. 53).

Loyalty may refer to one's intention to repeat uses of a service or purchases of a product, or willingness to recommend the service/product (Sur, 2011: p. 123); it may also represent a higher-order or long-term commitment, a psychological attachment of a person to an agent (Sur, 2011: p. 124). Therefore, loyalty may be understood as strong feelings of allegiance or commitments (Casaló, Flavián, & Guinalú, 2008: p. 328). Others argue that loyalty may refer to resistance to switch or willingness to give more (Faisal, Gonzalez-Rodriguez, Fernandez-Lanvin, & Andres-Suarez, 2017: p. 851). And it is strongly related to satisfaction, i.e. the pleasurable fulfillment of a need or a goal (Oliver, 1999: p. 34). Thus, loyalty involves preference, liking, and repeated episodes of intent to reuse a system (Jambulingam, Kathuria, & Nevin, 2011: 42). It is non-random behavior that includes a psychological link (Casaló, Flavián, & Guinalú, 2008: 328).

Familiarity could be regarded as a precondition of trust, since it can lead to an understanding of an agent's current actions and trust refers to beliefs about an agent's future actions (Luhmann, 1979: p. 19, 20, 73). It creates a framework and understanding of the environment, often based on previous interactions, experiences, and learning of what, why, where, and when agents do what they do (Gefen, 2000: p. 726-727). Lifelong experience has also been regarded as a precondition of trust as it may displace illusions and assumptions (McKnight, Cummings, & Chervany, 1998: p. 480, 483).

Reputation that may reflect professional competence (McKnight, Cummings, & Chervany, 1998: p. 480) has been defined as what is generally said or believed about an agent's standing; a quantity derived from the underlying system that may be globally visible (Jøsang, Ismail, & Boyd, 2007: p. 620; Butter, Liu, & Tan, 2010: p. 165). To some authors, reputation can resolve the problem of dealing with strangers (Resnick, Zeckhauser, Friedman, & Kuwabara, 2000). In this context, trust could depend on whether there are other parties who may assure the potential trustor that an agent is trustworthy. To some, trust has been linked to prediction and affection of behavior (Granovetter, 1973: p. 1374), but also to believing the source without independent evidence. Hence, reputation might not be enough. Performance within a given acceptable range may also be needed (Audi, 2008: p. 97).

Another trust-enhancing factor is explanation. People tend to trust more when others explain why they do what they do (Pieters, 2011: p. 53). Similarly, the levels of trust in a system are higher, when it can explain its processes and decisions (Sørmo, Cassens, & Aamodt, 2005). In fields of technology, authors have distinguished between several explanation goals, including transparency, justification, and relevance (Roth-Berghofer & Cassens, 2005: p. 454-456; Sørmo, Cassens, & Aamodt, 2005). The transparency goal means to understand how the system found an answer; it, thus, needs to explain how it reached a specific answer. Justification, explaining why the answer is a good answer, is said to increase confidence. And relevance, explaining why a question asked is relevant,

may justify the strategy pursued by the system (Roth-Berghofer & Cassens, 2005).

On the other hand, suspicion, distrust, errors, or lack of information have been regarded as factors that may diminish trust. Suspicion has been defined as a state, in which perceivers actively entertain multiple, plausibly rival, hypotheses about the motives or genuineness of an agent's behavior (Fein & Hilton, 1994: p. 168). So, one can be said to be suspicious of the occurrence of an event, if the disconfirmation of the expectation of the event's occurrence is preferred to its confirmation, and if the expectation of its occurrence leads to behavior that is intended to reduce its negative motivational consequences (Deutsch, 1958: p. 267). And distrust has been defined as a lack of confidence in an agent, a concern that the latter may act to harm, that the agent does not "care" about one's welfare, "intends" to act harmfully, or is hostile (Connelly, Zweig, Webster, & Trougakos, 2012: p. 68). Distrust may be engendered when an agent is perceived as not sharing key cultural values (Sitkin & Roth, 1993: p. 371). Moreover, machine errors may have a strong effect on trust; their magnitude is an important factor in loss of trust (Corritore, Kracher, & Wiedenbeck, 2003: p. 746). To some authors, diminishing trust could mean spoiling communications, making agreements unenforceable, undermining transitions, reducing solidarity (Schelling, 1965: p. 378), or making information unavailable (Pagden, 1988: p. 133-134)¹⁰.

While blockchains and, thus, cryptocurrencies are often referred to as *trustless* (Angel & McCabe, 2015: p. 605), this may not be quite accurate. It seems that trust has been shifted away from human actors and toward a cryptographic system; trust is most probably being depersonalized (Smolenski, 2018). And commentators could argue that trusting these systems would be abnormal; people normally trust other people (Vasilomanolakis, Wolf, Böck, Karuppayah, & Mühlhäuser, 2017).

Yet trust is an act of the trustor (Corritore, Kracher, & Wiedenbeck, 2003)¹¹. So, it could—to some extent—be put in the context of blockchains; this technology could be viewed as the object of trust (Corritore, Kracher, & Wiedenbeck, 2003: p. 739). Humans do trust that a given system will behave in a certain way. Perhaps, this is because they believe it to be more reliable (Mosier & Skitka, 1996). Namely, some see algorithms' products as a series of writing acts that may change our expectations of what may show up in the everyday world, acts that are given voice which is increasingly heard in everyday life and achieving presence as *local intelligence* (Thrift, 2005: p. 155). And people, trusting algorithms, become vulnerable to their effects. Whether as a resistance to traditional institutions (Appelbaum & Smith, 2018: p. 30) or as an evolution of humanity, trusting algorithms is an everyday practice. In case of Bitcoins, it has been argued that one does not have to trust Nakamoto, a bank, or any other person or institution;

¹⁰Pagden (1988: p. 133-134) refers to the Spaniards, who systematically reduced the amount of information available to the citizenry to destroy the *trusting society*.

¹¹Corritore, Kracher, & Wiedenbeck, (2003: 741) distinguish between trust, which is an act of the trustor, and trustworthiness, i.e. a characteristic of the object of trust.

one must simply trust the cryptographic algorithm (Maurer, Nelms, & Swartz, 2013: p. 264). As some have put it that we are now trusting systems to identify what we need to know is as momentous as having relied on credentialed experts, the scientific method, common sense, or the word of god (Gillespie, 2014: p. 168).

To draw some final conclusions, cryptology, the science behind cryptocurrencies (Genkin, Papadopoulos, & Papamantou, 2018: p. 78), is examined.

6. Cryptology: The Science behind Cryptocurrencies

Steganography and cryptology are two ways to keep secrets. Steganography hides the existence of the very message, e.g. secret ink. Cryptology transforms the message into something unintelligible that the “enemy” will have no hope of reading (Dooley, 2013: p. 4-12). Cryptology performs a transformation, known as the “plaintext”, which produces a new version of the message, the “ciphertext”¹² (Kittler, 2008). The process is “encoding” or “enciphering” the plaintext; the message in ciphertext is the “cryptogram”. To reverse the process, the system performs an inverse transformation, called “decoding” or “decrypting” the ciphertext (Dooley, 2013).

For instance, the word “stop” could be transformed into “XAVW”, provided that s = X, t = A, o = V and p = W.

Cryptology comes from the Greek word “*kryptós*” (“*κρυπτός*”) that means “hidden” or “secret” (Gómez Pardo, 2013: p. xxv). It is known to have existed for close to 2,500 years (Dooley, 2013: p. 4). The social need for privacy, but also the need to overcome concerns (Walton, 2006: p. 69), led to this study that involves secret writing (Dooley, 2013). Cryptology has been defined as the science of dealing with the protection of information and computation using mathematical techniques (Kahn, 1967).

While its origins are rooted in antiquity, when political leaders, or later governments, used it to protect their secrets, the subject has experienced explosive growth since the middle of the 20th century (Gómez Pardo, 2013: p. v; Walton, 2006: p. 70-71). It has been adopted by the private sector; firms needed to protect information in digital form and provide security services, due to the proliferation of computers and communications systems in the 1960s (Menezes, Oorschot, & Vanstone, 1996: p. 1). Cryptology allowed Julius Caesar to use cipher and send messages to friends and political allies; by changing the order of the letters not a word could be made out (Dooley, 2013: p. 11-12). Similarly, this science enables a bank to know that it really is Bill Gates requesting from his laptop in Fiji a transfer of 10,000,000,000 U.S. dollars (Menezes, Oorschot, & Vanstone, 1996: p. xxi). And, today, it is being used by almost everyone on a daily basis, when e.g. connecting to a Wi-Fi network or using a Web browser (Gómez Pardo, 2013: p. v).

Cryptology could be regarded as a battle between cryptographers and crypta-

¹²Cipher was another name for the zero that reached Europe from India *via* Baghdad and put *sifī* (Arabic: “emptiness”) into mathematical-technical power (Kittler, 2008: p. 42).

¹³From a mathematical perspective, encryption has been defined as “a mapping of a finite set of symbols of an alphabet onto a suitable signal sequence” (Kittler, 2008: p. 40).

analysts; it embraces cryptography and cryptanalysis (Kahn, 1967). The former is the actual securing, control, and identification of information; it deals with the design of “good” encryption¹³ schemes (Gómez Pardo, 2013: p. xxviii; Kittler, 2008). The latter is quite the opposite; it is made up of all the attempts one may develop to break these schemes, to undermine, circumvent and/or break what cryptography is attempting to accomplish (Mertz, 2001: p. 1-2). Cryptanalysis may be passive, e.g. eavesdropping, or active, e.g. tampering with ciphertexts in a channel (Gómez Pardo, 2013: p. xxix). And it is essential to cryptography in a negative sense; to prove that the cryptographic steps are worthwhile, cryptanalysis must fail (Mertz, 2001: p. 2).

Focusing on cryptography, it studies mathematical techniques related to aspects of information security (Menezes, Oorschot, & Vanstone, 1996). Its goals and, thus, its potential “security properties”, may include confidentiality, integrity, authentication and non-repudiation (Chin, 1999: p. 33; Menezes, Oorschot, & Vanstone, 1996: p. 4). More precisely, confidentiality (including secrecy) is a service to keep the items of information from all but those authorized to have them or to know who can read the data. Integrity is a service to address unauthorized alteration, to detect corruption of data; one may obtain assurance that the message sent by an agent has not been altered by a third party (Gómez Pardo, 2013: p. xxvii). Authentication is related to identification, knowing the identity of an agent or process involved; this means that, when X receives a message from Y, X knows that it is really Y who sent the message (Gómez Pardo, 2013: p. xxvii). Non-repudiation is a service that prevents an agent from denying previous commitments or actions (Menezes, Oorschot, & Vanstone, 1996: p. 4); after sending a message to X, Y cannot claim that she did not send it.

In this context, cryptography has been understood as a technique to manage secrecy (Phillips, 1998: p. 244) or to guarantee confidentiality, to hide information from outsiders (Kahn, 1967). Aiming to prevent and detect cheating or other malicious activities, cryptography could be a way to enhance trust. Although it may not directly create trust, it can help enforce the policies that underpin and promote trust in various ways (Walton, 2006: p. 71). So, cryptocurrencies, based on blockchains and cryptology, could –to some extent– meet some of the above discussed trust-enhancing factors.

To place trust in the context of cryptocurrencies, one could argue that, in many cases, they may implement the necessary techniques to ensure transaction security (Rowe, 2017; Yin, Wen, Li, Zhang, & Jin, 2018; Puthal, Malik, Mohanty, Kougianos, & Yang, 2018). Namely, by using encryption, hash functions, digital signatures, certification, and authorization (Chin, 1999: p. 34; Menezes, Oorschot, & Vanstone, 1996), some transaction security could be guaranteed. So, some levels of *competence* could be met; a user may perceive the expertise of the very network, which could properly perform its function.

Credibility could also be met, since authors have argued for blockchains’ capability to perform both effectively and reliably (Muzammal, Qu, & Nasrulin, 2019; Appelbaum & Smith, 2018: p. 36; Ichikawa, Kashiyama, & Ueno, 2017).

Users may strongly believe that the very network can have the “*expertise and skill*” to perform its role. As authors have argued, blockchain’s characteristics that could support users’ credibility may include the honesty that decentralization and public ledger’s transparency may ensure, but also the expertise supported by miners’ competence and hard labor (Sas & Khairuddin, 2017: p. 6506). To some, users may trust the code, because such decentralization and the public-key encryption of users’ identities are hardwired into the system (Lustig & Nardi, 2015: p. 745).

As regards *predictability*, the expectation that future transactions will be successfully completed with *consistency*, some blockchains are believed to be capable of acting consistently (Decker, Seidel, & Wattenhofer, 2014; Tseng, 2017; Chen, Zhao, Wang, Zhang, & Cui, 2018). And consistency, allowing users to efficiently fulfill tasks (Hof, 2015), reflects ease of use. The latter is suggested as a *security property* of cryptography (Kobeissi & Breault, 2013); so, the cryptographic protocol may support predictability (Sas & Khairuddin, 2017: p. 6506).

Authors have suggested models to achieve high levels of *integrity* (Zikratov, Kuzmin, Akimenko, Niculichev, & Yalansky, 2017; Liu, Yu, Chen, Xu, & Zhu, 2017); thus, the aspect of *honesty* could be addressed. Besides, digital signatures, the electronic analog of written signatures, are being used to achieve the above *security* goals of cryptography that include integrity, the service to address unauthorized alteration of information (Gómez Pardo, 2013: p. xxvii).

Moreover, it has been argued that algorithms are perceived to have higher levels of *fairness*, since they follow the same procedures every time, they are not influenced by emotional factors and have no agency. Hence, they could be perceived less biased than human decision-makers (Lee, 2018: p. 4). In case of blockchains, smart contracts have been proposed to establish fairness (Danzi, Angelichinoski, Stefanović, & Popovski, 2017; Heilman, Baldimtsi, & Goldberg, 2016). The latter could –to a certain extent– be met, since cryptography may allow an agent to get a copy of data if and only if another agent gets one (Jamroga, Melissen, & Schnoor, 2014: p. 24). Furthermore, fair-exchange protocol schemes have been suggested to ensure that e.g. an honest party engaged in a transaction does not get penalized, when a dishonest party misbehaves (Jayasinghe, Markantonakis, & Mayes, 2014: p. 45; Bentov & Kumaresan, 2014). But, to many authors, the *unbiased-argument* is an unsustainable belief and this has been shown by prior work (Friedman & Nissenbaum, 1996). The claim that algorithms decide more objectively cannot always be taken at face value, when human judgement may be built-in (Burrell, 2016: p. 3). In case of cryptocurrencies, some have observed further limitations in delivering fairness (Liu, Li, Karame, & Asokan, 2016: p. 2; Gürçan, Pozzo, & Tucci-Piergiovanni, 2017). Namely, some protocols do not provide fairness, when the majority of the parties is dishonest (Kumaresan, Vaikuntanathan, & Vasudevan, 2016: p. 406-407; Andrychowicz, Dziembowski, Malinowski, & Mazurek, 2014: p. 444, 447).

As regards *benevolence*, which involves concern for the well-being or care and goodwill, it would most probably be hard to argue for cryptocurrencies’ “*kind-*

ness” or their “*altruism*” that would reduce people’s uncertainty. Talking about the ethics of machines might be like speaking of the happiness of water (Castell, 2018: p. 743). Yet, benevolence also refers to perceptions of an agent’s efforts to achieve some value that is desirable. And some authors have argued for the potential ethical impact of cryptocurrencies as beneficial, detrimental, and ambiguous (Dierksmeier & Seele, 2018; Meyer & Hudon, 2018: p. 10; Novak, 2018).

Loyalty, as intentions to repeated uses of cryptocurrencies, could perhaps be met, as some scholars argue for an expressed enthusiasm (Li & Wang, 2017: p. 49; Peck, 2017: p. 28); many merchants accept cryptocurrencies as an excellent medium of exchange (Andreessen, 2014; Pangas & Park, 2017: p. 16). But some time would most probably be needed to observe their long-term acceptance, use, and people’s commitment to them. And this may also be the case concerning *familiarity*, which might require lifelong *experience*.

Reputation, what is generally said or believed about cryptocurrencies’ standing, is a hotly debated topic. They have been associated with illegal activities (Kewell, Adams, & Parry, 2017; Ramey, 2018); among the most critical issues are said to be black market transactions of weapons used in terrorist attacks, drugs, or child pornography (Seele, 2018: p. 134). However, reputation could be supported by large companies’ interest in cryptocurrencies (Sas & Khairuddin, 2017: p. 6506), which could bring massive benefits to consumers (Nguyen, 2016: p. 51). Being admittedly promising, they could disrupt the disruptors (Huckle, Bhattacharya, White, & Beloff, 2016), like Airbnb. Although models have already been proposed to achieve some high levels of good reputation (Truong, Um, Zhou, & Lee, 2018), perhaps, again, time might be needed to establish them.

Furthermore, these mechanisms may be capable of providing *explanations* as regards their decisions and processes. And authors have proposed such systems. For instance, instead of rejecting an unauthorized transaction or query, systems could provide a concise explanation of why the transaction or the query was rejected and what additional permissions one would need to be granted for a successful execution (Bender, Kot, & Gehrke, 2014). Such explanations could be provided by the system itself to achieve the goals of transparency, justification, and relevance (Roth-Berghofer & Cassens, 2005; Sørmo, Cassens, & Aamodt, 2005). The user could, then, understand e.g. how the system found an answer; and this would most probably increase and maintain trust (Pieters, 2011: p. 55; Gunning, 2017).

And, as regards factors that diminish trust, commentators could argue that *suspicion* and *distrust*, as lack of confidence or a concern that intentions are harmful, could emerge due to attacks (Eyal & Sirer, 2018). To some, cryptocurrencies, like Bitcoin, have an undeniable history of breaches and hacks (Angel & McCabe, 2015: p. 606); unfortunate events linked directly to their use and abuse by people (Umeh, 2016)¹⁴.

¹⁴Umeh (2016: p. 61) argues that the overall strength of any chain resides in the weakest link, which would probably be found in end-users of blockchains.

Scholars have also argued that *errors* might occur (Chepurnoy & Rathee, 2018). And their magnitude could be an important factor in loss of trust. Besides, in the absence of an intermediary, the latter's services would be eliminated; and these services could include error correction (Morse, 2018: p. 949-952).

However, *making information unavailable* is often not a feature of cryptocurrencies; the distributed nature and data integrity enable members to transact with a high degree of confidence based on the information available from the blockchain. Therefore, they tend to have more information available (Francisco & Swanson, 2018; Peck, 2016: p. 12). This could enhance trust.

7. Conclusion

So far, ICOs' basic properties have been examined to understand their function and detect some rights and obligations derived from tokens. It has been argued that while in some jurisdictions certain tokens may be treated as securities, in many cases they remain unregulated and, thus, several risks may be posed. A brief analysis of the shift from traditional mechanisms to blockchain has been provided to obtain a reasonably complete picture of the evolution of some "money mechanisms". And an overview on the multiple facets of trust and its enhancing and diminishing factors has allowed putting trust in the context of cryptocurrencies. Finally, cryptology's goals and potential properties have been discussed to examine cryptocurrencies' potential to enhance trust; even though they may not directly create trust, albeit they could help enforce the policies that promote trust.

It has been found that several trust-enhancing factors could—to a certain extent—be met, but some trust-diminishing aspects might also emerge. It seems that cryptocurrencies' true potential to be trusted may become apparent only many years after they are massively adopted. As regards the claim that these systems are *trustless*, in our opinion trust has most probably been shifted towards non-human agents. These agents could in some cases perform their role as objects of trust. As some have put it, trust can be earned or *promised*, but it cannot be ordered (Lieberman, 1983: p. 134). And cryptocurrencies could, at least to a certain extent, *promise* trust; perhaps, they could assure that their evaluations are fair and accurate, free from subjectivity, error or attempted influence (Gillespie, 2014: p. 179). Hence, it seems that some minimum levels of trust could be *promised* by the very network.

This might be the case, if designers and experts, who deal with crypto-coins, embedded the above trust-enhancing factors within the very heart design specifications of these technologies. Namely, decentralization and public-key encryption of users' identities may be hardwired into the systems (Lustig & Nardi, 2015: p. 745); this could lead to honesty or credibility. Other trust-enhancing parameters could also be embedded and hardwired. Scientists, focusing on such desirable and ideal properties (Zhang & Preneel, 2017: p. 280, 281), could also detect current weaknesses and avoid trust-diminishing aspects, e.g. making networks and information *invisible* (Pieters, 2011: p. 56).

In this context, systems could be designed to convey some meaningful information, some signals of trust-enhancing aspects, to people, the under-informed party (Butter, Liu, & Tan, 2012: p. 270, 272). By implementing such strategies, perhaps, cryptocurrencies could turn people into potential *crypto millionaires* (Thompson, 2018: p. 14), into coins' stakeholders who would be able to trust the very technology (Sas & Khairuddin, 2017: p. 6500).

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

- Abgaryan, A., Liu, L., Menteshashvili, T., Abgaryan, S., & Gao, C. (2017). *Aimwise: Decentralized ICO Servicing Platform. White Paper*.
<http://os4tp6h8i.bkt.cloudn.com/aimwiseWhitePaper.pdf>
- Abramovitch, R., Freedman, J., & Pliner, P. (1991). Children and Money: Getting an Allowance, Credit versus Cash, and Knowledge of Pricing. *Journal of Economic Psychology*, 12, 27-45. [https://doi.org/10.1016/0167-4870\(91\)90042-R](https://doi.org/10.1016/0167-4870(91)90042-R)
- Acres, W. M. (1931). *The Bank of England from Within: 1694-1900* (2nd ed.). London, England: The Oxford University Press.
- Adams, J. (2002). *Risk*. London, New York: Taylor & Francis (e-Library).
<https://doi.org/10.4324/9780203498965>
- Adhami, S., Giudici, G., & Martinazzi, S. (2018). Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings. *Journal of Economics and Business*. (Forthcoming) <https://doi.org/10.1016/j.jeconbus.2018.04.001>
- Adler, P. (2001). Market, Hierarchy, and Trust: The Knowledge Economy and the Future of Capitalism. *Organization Science*, 12, 215-234.
<http://www-bcf.usc.edu/~padler/research/MHT-1.pdf>
<https://doi.org/10.1287/orsc.12.2.215.10117>
- Ahern, K., Daminelli, D., & Fracassi, C. (2015). Lost in Translation? The Effect of Cultural Values on Mergers around the World. *Journal of Financial Economics*, 117, 165-189.
<https://doi.org/10.1016/j.jfineco.2012.08.006>
- Alesina, A., & Ferrara, E. (2002). Who Trusts Others? *Journal of Public Economics*, 85, 207-234. [https://doi.org/10.1016/S0047-2727\(01\)00084-6](https://doi.org/10.1016/S0047-2727(01)00084-6)
- Aljukhadar, M., Senecal, S., & Ouellette, D. (2010). Can the Media Richness of a Privacy Disclosure Enhance Outcome? A Multifaceted View of Trust in Rich Media Environments. *International Journal of Electronic Commerce*, 14, 103-126.
<https://www.jstor.org/stable/20749982>
<https://doi.org/10.2753/JEC1086-4415140404>
- Altman, I. (1973). Reciprocity of Interpersonal Exchange. *Journal of the Theory of Social Behavior*, 3, 249-261. <https://doi.org/10.1111/j.1468-5914.1973.tb00325.x>
- Andreessen, M. (2014). *Why Bitcoin Matters*. The New York Times.
<https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/>
- Andrychowicz, M., Dziembowski, S., Malinowski, D., & Mazurek, Ł. (2014). Secure Multiparty Computations on Bitcoin. In *2014 IEEE Symposium on Security and Privacy* (pp. 443-458). USA: IEEE. <https://ieeexplore.ieee.org/document/6956580>
<https://doi.org/10.1109/SP.2014.35>
- Angel, J., & McCabe, D. (2015). The Ethics of Payments: Paper, Plastic, or Bitcoin? *Jour-*

- nal of Business Ethics*, 132, 603-611. <https://doi.org/10.1007/s10551-014-2354-x>
- Appelbaum, D., & Smith, S. S. (2018). Blockchain Basics and Hands-On Guidance: Taking the Next Step toward Implementation and Adoption. *The CPA Journal*, 88, 28-37. <https://www.cpajournal.com/category/magazine/june-2018-issue/>
- Appleby, J. O. (1976). Locke, Liberalism and the Natural Law of Money. *Past & Present*, 71, 43-69. <https://www.jstor.org/stable/650353>
<https://doi.org/10.1093/past/71.1.43>
- Arnoldi, J. (2010). Sense Making as Communication. *Soziale Systeme*, 16, 28-48. https://soziale-systeme.ch/pdf/SoSy_01_10_Arnoldi_www.pdf
<https://doi.org/10.1515/sosys-2010-0103>
- Arrow, K. (1974). *The Limits of Organization*. New York: W.W. Norton.
- Audi, R. (2008). Some Dimensions of Trust in Business Practices: From Financial and Product Representation to Licensure and Voting. *Journal of Business Ethics*, 80, 97-102. <https://www.jstor.org/stable/41219194>
<https://doi.org/10.1007/s10551-007-9435-z>
- Bachmann, R., & Kroeger, F. (2017). Trust, Power or Money: What Governs Business Relationships? *International Sociology*, 32, 3-20. <http://journals.sagepub.com/doi/pdf/10.1177/0268580916673747>
- Baier, A. C. (1994). *Moral Prejudices: Essays on Ethics*. Cambridge, Massachusetts: Harvard University Press.
- Barron, J. (2012). SWIFT-ICC Collaborate on "Electronic Letter of Credit". *Business Credit*, 114, 52. <http://connection.ebscohost.com/c/articles/73310159/swift-icc-collaborate-on-electronic-letter-credit>
- Barry, K. (2007). The Aesthetics of Paper Money: National Difference during the Period of Enlightenment and Romanticism. In *Scotland, Ireland, and the Romantic Aesthetic* (pp. 55-76). USA: Bucknell University Press.
- Bauer, P. C., & Fatke, M. (2014). Direct Democracy and Political Trust: Enhancing Trust, Initiating Distrust or Both? *Swiss Political Science Review*, 20, 49-69. <https://doi.org/10.1111/spsr.12071>
- Baumol, J. W. (1952). The Transactions Demand for Cash: An Inventory Theoretic Approach. *The Quarterly Journal of Economics*, 66, 545-556. <https://www.jstor.org/stable/1882104>
<https://doi.org/10.2307/1882104>
- Beckert, J. (2006). Trust and Markets. In *Handbook of Trust Research* (pp. 318-331). UK, USA: Edward Elgar.
- Bell, S. (2001). The Role of the State and the Hierarchy of Money. *Cambridge Journal of Economics*, 25, 149-163. <https://ideas.repec.org/a/oup/cambje/v25y2001i2p149-63.html>
<https://doi.org/10.1093/cje/25.2.149>
- Belleflamme, P., Lambert, T., & Schwienbacher, A. (2014). Crowdfunding: Tapping the Right Crowd. *Journal of Business Venturing*, 29, 585-609. <https://doi.org/10.1016/j.jbusvent.2013.07.003>
- Bender, G., Kot, L., & Gehrke, J. (2014). Explainable Security for Relational Databases. In *Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data* (pp. 1411-1422). USA: ACM. <https://dl.acm.org/citation.cfm?doid=2588555.2593663>
- Bento, N., Gianfrate, G., & Groppo, S. V. (2018). Do Crowdfunding Returns Reward Risk? Evidences from Clean-Tech Projects. *Technological Forecasting & Social Change*.

- (Forthcoming) <https://doi.org/10.1016/j.techfore.2018.07.007>
- Bentov, I., & Kumaresan, R. (2014). How to Use Bitcoin to Design Fair Protocols. In *Advances in Cryptology, CRYPTO 2014, Lecture Notes in Computer Science, 8617* (pp. 421-439). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-44381-1_24
- Berentsen, A., & Schär, F. (2018). A Short Introduction to the World of Cryptocurrencies. *Federal Reserve Bank of St. Louis Review First Quarter, 100*, 1-16. <https://doi.org/10.20955/r.2018.1-16>
- Biktimirov, M. R., Domashev, A. V., Cherkashin, P. A., & Shcherbakov, A. Y. (2017). Blockchain Technology: Universal Structure and Requirements. *Automatic Documentation and Mathematical Linguistics, 51*, 235-238. <https://doi.org/10.3103/S0005105517060036>
- Blanc, J. (1998). Free Money for Social Progress, Theory and Practice of Gesell's Accelerated Money. *The American Journal of Economics and Sociology, 57*, 469-483. <https://www.jstor.org/stable/3487118>
<https://doi.org/10.1111/j.1536-7150.1998.tb03376.x>
- Blau, P. M. (1964). *Exchange and Power in Social Life*. USA, UK: Transaction Publishers.
- Bok, S. (1978). *Lying: Moral Choice in Public and Private Life*. New York: Pantheon Books.
- Bottazzi, L., Rin, M., & Hellmann, T. (2016). The Importance of Trust for Investment: Evidence from Venture Capital. *The Review of Financial Studies, 29*, 2283-2318. <https://doi.org/10.1093/rfs/hhw023>
- Boyd, D. (2014). *What Is "Fairness"? What Happens When Technology Decides? The Message*. <https://medium.com/message/what-is-fairness-73940071840>
- Braun, B. (2016). Speaking to the People? Money, Trust, and Central Bank Legitimacy in the Age of Quantitative Easing. *Review of International Political Economy, 23*, 1064-1092. <https://doi.org/10.1080/09692290.2016.1252415>
- Bukspan, E. (2013). Trust and the Triangle Expectation Model in Twenty-First Century Contract Law. *DePaul Business and Commercial Law Journal, 11*, 379-415. <http://via.library.depaul.edu/bclj/vol11/iss3/4>
- Burger, C., Kuhlmann, A., Richard, P., & Weinmann, J. (2016). *Blockchain in the Energy Transition, a Survey among Decision-Makers in the German Energy Industry*. Berlin, Germany: Deutsche Energie-Agentur GmbH (dena)-German Energy Agency & ESMT European School of Management and Technology GmbH. http://static.esmt.org/publications/whitepapers/dena_esmt_study_blockchain_english_2016.pdf
- Burrell, J. (2016). How the Machine "Thinks": Understanding Opacity in Machine Learning Algorithms. *Big Data & Society, 3*, 1-12. <https://doi.org/10.1177/2053951715622512>
- Burt, R. S., & Knez, M. (1996). Ch. 5: Trust and Third-Party Gossip. In *Trust in Organizations: Frontiers of Theory and Research* (pp. 68-89). USA: SAGE. <https://doi.org/10.4135/9781452243610.n5>
- Buterin, V. (2013). *What Proof of Stake Is and Why It Matters*. Bitcoin Magazine. <https://bitcoinmagazine.com/articles/what-proof-of-stake-is-and-why-it-matters-1377531463/>
- Buterin, V. (2014). *Ethereum White Paper, a Next Generation Smart Contract & Decentralized Application Platform*. <https://coss.io/documents/white-papers/ethereum.pdf>
- Butler, J. K. (1991). Toward Understanding and Measuring Conditions of Trust: Evolution of a Condition of Trust Inventory. *Journal of Management, 17*, 643-663.

- <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.2423&rep=rep1&type=pdf>
- Butter, F. A. G., Liu, J., & Tan, Y.-H. (2010). Ch. 9: Using Trust and Reputation in Government to Business Relationships: The Authorized Economic Operator (AEO) as an Example. In *Breaking the Ice Between Government and Business: From IT-Enabled Control Procedure Redesign to Trusted Relationship Building* (pp. 155-184). Amsterdam: Thela Thesis/TI.
<https://research.vu.nl/ws/files/42189460/complete%20dissertation.pdf>
- Butter, F. A. G., Liu, J., & Tan, Y.-H. (2012). Using IT to Engender Trust in Government-to-Business Relationships: The Authorized Economic Operator (AEO) as an Example. *Government Information Quarterly*, 29, 261-274.
<https://doi.org/10.1016/j.giq.2011.05.004>
- Buyser De, K., Gajda, O., Kleverlaan, R., & Marom, D. (2012). *A Framework for European Crowdfunding*.
http://eurocrowd.winball2.de/wp-content/blogs.dir/sites/85/2013/06/Framework_EU_Crowdfunding.pdf
- Carlson, J., & Selin, A. (2018). Initial Coin Offerings: Recent Regulatory and Litigation Developments. *The Investment Lawyer*, 25, 18-30.
<https://www.mayerbrown.com/Initial-Coin-Offerings-Recent-Regulatory-and-Litigation-Developments-03-01-2018/>
- Carruthers, B. G., & Babb, S. (1996). The Color of Money and the Nature of Value: Greenbacks and Gold in Postbellum America. *American Journal of Sociology*, 101, 1556-1591. <https://www.jstor.org/stable/2782112>
<https://doi.org/10.1086/230867>
- Casaló, L., Flavián, C., & Guinalú, M. (2008). The Role of Perceived Usability, Reputation, Satisfaction and Consumer Familiarity on the Website Loyalty Formation Process. *Computers in Human Behavior*, 24, 325-345. <https://doi.org/10.1016/j.chb.2007.01.017>
- Casson, M. (1991). *The Economics of Business Culture: Game Theory, Transaction Costs, and Economic Performance*. Oxford: Clarendon Press.
- Castell, S. (2018). The Future Decisions of RoboJudge HHJ Arthur Ian Blockchain: Dread, Delight or Derision? *Computer Law & Security Review*, 34, 739-753.
<https://doi.org/10.1016/j.clsr.2018.05.011>
- Cerezo Sánchez, D. (2017). *An Optimal ICO Mechanism*. Munich Personal RePEc Archive. MPRA Paper No. 81285. <https://mpra.ub.uni-muenchen.de/81285/>
<https://doi.org/10.2139/ssrn.3040343>
- Chadha, J., & Newby, E. (2013). *Midas, Transmuting All, into Paper: The Bank of England and the Banque de France during the Revolutionary and Napoleonic Wars (Research Discussion Paper No. 20/2013)*. Finland: Bank of Finland.
<https://doi.org/10.2139/ssrn.2331310>
- Chen, X., Zhao, S., Wang, C., Zhang, S., & Cui, H. (2018). *GEEC: Scalable, Efficient, and Consistent Consensus for Blockchains*. Ithaca, New York: Cornell University.
<https://arxiv.org/abs/1808.02252>
- Chepurnoy, A., & Rathee, M. (2018). Checking Laws of the Blockchain with Property-Based Testing. In *Proceedings of the International Workshop on Blockchain Oriented Software Engineering* (pp. 40-47). Italy: IEEE. <https://ieeexplore.ieee.org/document/8327570>
- Child, J. (2001). Trust: The Fundamental Bond in Global Collaboration. *Organizational Dynamics*, 29, 274-288. [https://doi.org/10.1016/S0090-2616\(01\)00033-X](https://doi.org/10.1016/S0090-2616(01)00033-X)
- Chiles, T. H., & McMackin, J. F. (1996). Integrating Variable Risk Preferences, Trust, and

- Transaction Cost Economics. *The Academy of Management Review*, 21, 73-99.
<https://www.jstor.org/stable/258630>
<https://doi.org/10.5465/amr.1996.9602161566>
- Chin, S.-K. (1999). High-Confidence Design for Security: Don't Trust-Verify. *Communications of the ACM*, 42, 33-37. <https://dl.acm.org/citation.cfm?doid=306549.306560>
<https://doi.org/10.1145/306549.306560>
- Chown, J. (2003). *A History of Monetary Unions* (1st ed.). London, UK: Routledge.
<https://doi.org/10.4324/9780203417782>
- CJEU (2015). *Judgment of the Court of Justice of the European Union (Fifth Chamber) of 22 October 2015, Skatteverket v David Hedqvist, Case C-264/14, ECLI:EU:C:2015:718.*
- Clayton, J. (2017). *Governance and Transparency at the Commission and in Our Markets. Remarks at the PLI 49th Annual Institute on Securities Regulation.* New York: Securities and Exchange Commission.
<https://www.sec.gov/news/speech/speech-clayton-2017-11-08>
- Conheady, G. (2018). *The EU Approach to ICO Regulation: A Friendlier Regulatory Framework for ICOs? Bloomberg BNA. The Bureau of National Affairs.*
<https://www.bna.com/eu-approach-ico-n57982090582/>
- Conley, P. J. (2017). *Blockchain and the Economics of Crypto-Tokens and Initial Coin Offerings.* Nashville, TN: Vanderbilt University (Department of Economics Working Papers, VUECON-17-00008).
<http://www.accessecon.com/pubs/VUECON/VUECON-17-00008.pdf>
- Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. (2012). Knowledge Hiding in Organizations. *Journal of Organizational Behavior*, 33, 64-88.
<https://doi.org/10.1002/job.737>
- Conti, M., & Kumar, S. (2017). *A Survey on Security and Privacy Issues of Bitcoin.*
<https://arxiv.org/pdf/1706.00916.pdf>
- Corbet, S., Lucey, B., & Yarovaya, L. (2018). Datestamping the Bitcoin and Ethereum Bubbles. *Finance Research Letters*, 26, 81-88. <https://doi.org/10.1016/j.frl.2017.12.006>
- Corré, I. J. (2000). Reconciling the Old Theory and the New Evidence: Comments on Ronald Mann's the Role of Letters of Credit in Payment Transactions. *Michigan Law Review*, 98, 2548-2553. <https://www.jstor.org/stable/i255164>
<https://doi.org/10.2307/1290354>
- Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-Line Trust: Concepts, Evolving Themes, a Model. *International Journal of Human-Computer Studies*, 58, 737-758.
[https://doi.org/10.1016/S1071-5819\(03\)00041-7](https://doi.org/10.1016/S1071-5819(03)00041-7)
- Currall, S. C., & Inkpen, A. C. (2006). On the Complexity of Organizational Trust: A Multi-Level Co-Evolutionary Perspective and Guidelines for Future Research. In *Handbook of Trust Research* (pp. 235-246). UK, USA: Edward Elgar.
- Currall, S., & Judge, T. (1995). Measuring Trust between Organizational Boundary Role Persons. *Organizational Behavior and Human Decision Processes*, 64, 151-170.
<https://doi.org/10.1006/obhd.1995.1097>
- Danzi, P., Angjelichinoski, M., Stefanović, C., & Popovski, P. (2017). Distributed Proportional-Fairness Control in MicroGrids via Blockchain Smart Contracts. In *Proceedings of the International Conference on Smart Grid Communications* (pp. 45-51). Germany: IEEE. <https://ieeexplore.ieee.org/document/8340713>
- Dasgupta, P. (1988). Ch. 4: Trust as a Commodity. In *Trust: Making and Breaking Cooperative Relations* (pp. 49-72). Great Britain: Basil Blackwell.
https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20c

[operative%20relations.pdf](#)

- Davenport, E., Dibben, M., Friedman, B., Marsh, S., Rosenbaum, H., & Thimbleby, H. (2000). Non-Contractual Trust, Design, and Human and Computer Interactions. In *Proceedings CHI'00 Extended Abstracts on Human Factors in Computing Systems* (pp. 239-240). The Hague, The Netherlands: ACM.
- Davies, G. (2002). *A History of Money: From Ancient Times to the Present Day* (3rd ed.). Cardiff, Wales: University of Wales Press.
http://library.uniteddiversity.coop/Money_and_Economics/A_History_of_Money-From_Ancient_Times_to_the_Present_Day.pdf
- Decker, C., Seidel, J., & Wattenhofer, R. (2014). *Bitcoin Meets Strong Consistency*. Ithaca, New York: Cornell University. <https://arxiv.org/abs/1412.7935>
- Desan, C. (2014). Ch. 8: Reinventing Money, The Beginning of Bank Currency. In *Making Money: Coin, Currency, and the Coming of Capitalism* (pp. 295-329). Great Britain: Oxford University Press.
- Desmet, P., Cremer, D., & Dijk, E. (2011). In Money We Trust? The Use of Financial Compensations to Repair Trust in the Aftermath of Distributive Harm. *Organizational Behavior and Human Decision Processes*, 114, 75-86.
<https://doi.org/10.1016/j.obhdp.2010.10.006>
- Deutsch, M. (1958). Trust and Suspicion. *The Journal of Conflict Resolution*, 2, 265-279.
<https://www.jstor.org/stable/172886>
<https://doi.org/10.1177/002200275800200401>
- Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and Business Ethics. *Journal of Business Ethics*, 152, 1-14. <https://doi.org/10.1007/s10551-016-3298-0>
- Dobrin, A. (2012). *It's Not Fair! But What Is Fairness? Three Different Ideas of Fairness: Sameness, Deservedness, and Need*. Psychology Today.
<https://www.psychologytoday.com/intl/blog/am-i-right/201205/its-not-fair-what-is-fairness>
- Dooley, J. F. (2013). *A Brief History of Cryptology and Cryptographic Algorithms*. New York, London: Springer. <https://doi.org/10.1007/978-3-319-01628-3>
- Dunn, J. (1988) Ch. 5: Trust and Political Agency. In *Trust: Making and Breaking Cooperative Relations* (pp. 73-93). Great Britain: Basil Blackwell.
https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf
- Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an Experience Technology. *Information, Communication & Society*, 9, 433-451.
<https://doi.org/10.1080/13691180600858606>
- Economist (2015). *The Promise of the Blockchain: The Trust Machine*.
<https://www.economist.com/leaders/2015/10/31/the-trust-machine>
- Egger, F. N. (2001). Affective Design of E-Commerce User Interfaces: How to Maximise Perceived Trustworthiness. In *Proceedings of the International Conference on Affective Human Factors Design* (pp. 317-324). New York: ACM Press.
- ESMA (2017). *Statement: ESMA Alerts Firms Involved in Initial Coin Offerings (ICOs) to the Need to Meet Relevant Regulatory Requirements*. Paris, France: European Securities and Markets Authority.
https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf
- European Central Bank (2012). *Virtual Currency Schemes*. Frankfurt am Main, Germany: European Central Bank.

- <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>
- European Central Bank (2015). *Virtual Currency Schemes: A Further Analysis*. Frankfurt am Main, Germany: European Central Bank.
- <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
- Europol (2015). *Why Is Cash Still King? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator for Money Laundering*. EU: European Police Office.
- Eyal, I., & Sirer, E. G. (2018). Majority Is Not Enough: Bitcoin Mining Is Vulnerable. *Communications of the ACM*, 61, 95-102. <https://dl.acm.org/citation.cfm?id=3212998>
<https://doi.org/10.1145/3212998>
- Faisal, N. C. M., Gonzalez-Rodriguez, M., Fernandez-Lanvin, D., & Andres-Suarez, J. (2017). Web Design Attributes in Building User Trust, Satisfaction, and Loyalty for a High Uncertainty Avoidance Culture. *IEEE Transactions on Human-Machine Systems*, 47, 847-859. <https://ieeexplore.ieee.org/document/7742992>
<https://doi.org/10.1109/THMS.2016.2620901>
- Federal Reserve Board (2016). *The Federal Reserve Payments Study 2016*. A Federal Reserve System Publication.
- <https://www.federalreserve.gov/newsevents/press/other/2016-payments-study-20161222.pdf>
- Fein, S., & Hilton, J. L. (1994). Judging Others in the Shadow of Suspicion. *Motivation and Emotion*, 18, 167-198. <https://doi.org/10.1007/BF02249398>
<https://pdfs.semanticscholar.org/2ea0/b90fd5dc44b0cf1304377558d355fee0ef8c.pdf>
- Fenu, G., Marchesi, L., Marchesi, M., & Tonelli, R. (2018). The ICO Phenomenon and Its Relationships with Ethereum Smart Contract Environment. In *Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)* (pp. 26-32). Campobasso, Italy: IEEE.
- <https://arxiv.org/ftp/arxiv/papers/1803/1803.01394.pdf>
- Financial Action Task Force (2014). *FATF Report, Virtual Currencies, Key Definitions and Potential AML/CFT Risks*. Paris, France: FATF/OECD.
- <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf>
- Findlay, C. (2017). Participatory Cultures, Trust Technologies and Decentralisation: Innovation Opportunities for Recordkeeping. *Archives and Manuscripts*, 45, 176-190.
- <https://doi.org/10.1080/01576895.2017.1366864>
- FINMA (2018). *Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs)*. Bern, Switzerland: Swiss Financial Market Supervisory Authority. <https://www.finma.ch/en/>
- Fogg, B. J., & Tseng, H. (1999). The Elements of Computer Credibility. In *CHI'99 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 80-87). New York: ACM. <https://dl.acm.org/citation.cfm?doid=302979.303001>
<https://doi.org/10.1145/302979.303001>
- Fogg, B. J., Marshall, J., Kameda, T., Solomon, J., Rangnekar, A., Boyd, J., et al. (2001). Web Credibility Research: A Method for Online Experiments and Early Study Results. In *CHI EA'01 Extended Abstracts on Human Factors in Computing Systems* (pp. 295-296). New York: ACM. <https://dl.acm.org/citation.cfm?doid=634067.634242>
<https://doi.org/10.1145/634067.634242>
- Francisco, K., & Swanson, D. (2018). The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency. *Logistics*, 2, 1-13.
- <https://doi.org/10.3390/logistics2010002>

- Frankel, T. (1983). Fiduciary Law. *California Law Review*, 71, 795-836.
<https://scholarship.law.berkeley.edu/californialawreview/vol71/iss3/1/>
<https://doi.org/10.2307/3480303>
- Friedman, B., & Nissenbaum, H. (1996). Bias in Computer Systems. *ACM Transactions on Information Systems*, 14, 330-347. <https://doi.org/10.1145/230538.230561>
<https://dl.acm.org/citation.cfm?doid=230538.230561>
- Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*. USA: Free Press.
- Funk, E., Riddell, J., Ankel, F., & Cabrera, D. (2018). Blockchain Technology: A Data Framework to Improve Validity, Trust, and Accountability of Information Exchange in Health Professions Education. *Academic Medicine*, 93, 1-17.
<https://doi.org/10.1097/ACM.0000000000002326>
<https://insights.ovid.com/crossref?an=00001888-900000000-97880>
- Gambetta, D. (1988). Ch. 13: Can We Trust Trust? In *Trust: Making and Breaking Cooperative Relations* (pp. 213-237). Great Britain: Basil Blackwell.
https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf
- Ganesan, S. (1994). Determinants of Long-Term Orientation in Buyer-Seller Relationships. *Journal of Marketing*, 58, 1-19. <https://www.jstor.org/stable/1252265>
<https://doi.org/10.1177/002224299405800201>
- García-Marzá, D. (2005). Trust and Dialogue: Theoretical Approaches to Ethics Auditing. *Journal of Business Ethics*, 57, 209-219. <https://www.jstor.org/stable/25123470>
<https://doi.org/10.1007/s10551-004-8202-7>
- Gefen, D. (2000). E-commerce: The Role of Familiarity and Trust. *Omega*, 28, 725-737.
[https://doi.org/10.1016/S0305-0483\(00\)00021-9](https://doi.org/10.1016/S0305-0483(00)00021-9)
- Gefen, D., & Straub, D. W. (2004). Consumer Trust in B2C E-Commerce and the Importance of Social Presence: Experiments in E-Products and E-Services. *Omega*, 32, 407-424. <https://doi.org/10.1016/j.omega.2004.01.006>
- Genkin, D., Papadopoulos, D., & Papamanthou, C. (2018). Privacy in Decentralized Cryptocurrencies. *Communications of the ACM*, 61, 78-88.
<https://doi.org/10.1145/3132696>
<https://dl.acm.org/citation.cfm?doid=3229066.3132696>
- GFSC (2017). Statement on Initial Coin Offerings. Gibraltar: The Gibraltar Financial Services Commission. <http://www.fsc.gi/news/statement-on-initial-coin-offerings-250>
- Gibraltar Finance (2018). *Token Regulation, Proposals for the Regulation of Token Sales, Secondary Token Market Platforms, and Investment Services Relating to Tokens*. Gibraltar: Gibraltar Finance Centre, HM Government of Gibraltar.
<http://gibraltarfinance.gi/20180309-token-regulation---policy-document-v2.1-final.pdf>
- Giddens, A. (1990). *The Consequences of Modernity*. Stanford, CA: Stanford University Press.
- Gillespie, T. (2014). Ch. 9: The Relevance of Algorithms. In *Media Technologies: Essays on Communication, Materiality, and Society* (pp. 167-193). Cambridge, Massachusetts: MIT Press Scholarship Online.
<http://mitpress.universitypressscholarship.com/view/10.7551/mitpress/9780262525374.001.0001/upso-9780262525374-chapter-9>
- Gillette, C. P. (2000). Letters of Credit as Signals: Comments on Ronald Mann's "The Role of Letters of Credit in Payment Transactions". *Michigan Law Review*, 98, 2537-2547.
<https://www.jstor.org/stable/1290353>

- <https://doi.org/10.2307/1290353>
- Glaeser, E. L., Laibson, D. I., Scheinkman, J. A., & Soutter, C. L. (2000). Measuring Trust. *The Quarterly Journal of Economics*, 811-846.
<https://doi.org/10.1162/003355300554926>
https://scholar.harvard.edu/files/laibson/files/measuring_trust.pdf
- Gómez Pardo, J. L. (2013). *Introduction to Cryptography with Maple*. Berlin: Springer.
<https://doi.org/10.1007/978-3-642-32166-5>
- Good, D. (1988). Ch. 3: Individuals, Interpersonal Relations, and Trust. In *Trust: Making and Breaking Cooperative Relations* (pp. 31-48). Great Britain: Basil Blackwell.
https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf
- Grabner-Kräuter, S., & Kaluscha, E. A. (2003). Empirical Research in On-Line Trust: A Review and Critical Assessment. *International Journal of Human-Computer Studies*, 58, 783-812. [https://doi.org/10.1016/S1071-5819\(03\)00043-0](https://doi.org/10.1016/S1071-5819(03)00043-0)
- Granovetter, M. S. (1973). The Strength of Weak Ties. *American Journal of Sociology*, 78, 1360-1380. <https://www.jstor.org/stable/2776392>
<https://doi.org/10.1086/225469>
- Gray, F. (2017). *Crypto-Currency: Risky as Hell But Worth a Punt*. The Spectator.
<https://www.spectator.co.uk/2017/09/crypto-currencies-are-risky-as-hell-but-worth-a-punt/>
- Grüschow, R. M., Kemper, J., & Brettel, M. (2016). How Do Different Payment Methods Deliver Cost and Credit Efficiency in Electronic Commerce? *Electronic Commerce Research and Applications*, 18, 27-36. <https://doi.org/10.1016/j.elerap.2016.06.001>
- Guiso, L., Sapienza, P., & Zingales, L. (2009). Cultural Biases in Economic Exchange? *The Quarterly Journal of Economics*, 124, 1095-1131.
<https://doi.org/10.1162/qjec.2009.124.3.1095>
- Gunning, D. (2017). *Explainable Artificial Intelligence (XAI), DARPA/I2O*.
<https://www.darpa.mil/attachments/XAIProgramUpdate.pdf>
- Gürçan, Ö., Pozzo, A., & Tucci-Piergiovanni, S. (2017). On the Bitcoin Limitations to Deliver Fairness to Users. In *On the Move to Meaningful Internet Systems—OTM 2017 Conferences—Lecture Notes in Computer Science, 10573* (pp. 589-606). Cham: Springer.
https://doi.org/10.1007/978-3-319-69462-7_37
- Hacker, P. & Thomale, C. (2017). Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law. *European Company and Financial Law Review*. (Forthcoming) <https://doi.org/10.2139/ssrn.3075820>
- Halpin, R., & Moore, R. (2009). Developments in Electronic Money Regulation—The Electronic Money Directive: A Better Deal for E-Money Issuers? *Computer Law & Security Review*, 25, 563-568. <https://doi.org/10.1016/j.clsr.2009.09.010>
- Hammi, M. T., Hammi, B., Bellot, P., & Serhrouchni, A. (2018). Bubbles of Trust: A Decentralized Blockchain-Based Authentication System for IoT. *Computers & Security*, 78, 126-142. <https://doi.org/10.1016/j.cose.2018.06.004>
- Hartmann, F., Wang, X., & Lunesu, M. I. (2018). Evaluation of Initial Cryptoasset Offerings: The State of the Practice. In *Proceedings of the 2018 International Workshop on Blockchain Oriented Software Engineering, IWBOSE* (pp. 33-39). Italy: IEEE.
<https://ieeexplore.ieee.org/document/8327569>
- Heilman, E., Baldimtsi, F., & Goldberg, S. (2016). Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions. In *Financial Cryptography and Data Security: FC 2016 International Workshops BITCOIN, VOTING, and WAHC*

- Christ Church, Barbados, February 26, 2016—Revised Selected Papers* (pp. 43-60). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-662-53357-4_4
- Herland, M. (1977). "Perpetuum mobile" et Crédit Gratuit, Deux Propositions Oubliées Pour Améliorer le Fonctionnement d'une Économie Monétaire. *Revue Économique*, 28, 938-973. <http://monnaie-leman.org/wp-content/uploads/2015/10/Herland.pdf>
- Hof, H.-J. (2015). *User-Centric IT Security: How to Design Usable Security Mechanisms*. Ithaca, New York: Cornell University. <https://arxiv.org/abs/1506.07167>
- Hosmer, L. T. (1995). Trust: The Connecting Link between Organizational Theory and Philosophical Ethics. *The Academy of Management Review*, 20, 379-403. <https://www.jstor.org/stable/258851>
<https://doi.org/10.5465/amr.1995.9507312923>
- Hoy, M. (2017). An Introduction to the Blockchain and Its Implications for Libraries and Medicine. *Medical Reference Service Quarterly*, 36, 273-279. <https://doi.org/10.1080/02763869.2017.1332261>
- Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of Things, Blockchain and Shared Economy Applications. *Procedia Computer Science*, 98, 461-466. <https://doi.org/10.1016/j.procs.2016.09.074>
- Huggins, E. C. (2012). Reducing Ambiguity or Increasing Contracting Costs? Interpreting UCP 600 Article 16 Obligations and Fortis Bank v. Indian Overseas. *George Mason Journal of International Commercial Law*, 3, 312-338. http://www.georgemasonjicl.org/wp-content/uploads/2012/06/HUGGINS_3_J_Intl_Co_m_Law_312.pdf
- Iansiti, M., & Lakhani, K. (2017). The Truth about Blockchain. *Harvard Business Review*, 1-11. https://enterpriseproject.com/sites/default/files/the_truth_about_blockchain.pdf
- Ichikawa, D., Kashiyama, M., & Ueno, T. (2017). Tamper-Resistant Mobile Health Using Blockchain Technology. *JMIR Health & Health*, 5, e111. <https://mhealth.jmir.org/2017/7/e111/>
<https://doi.org/10.2196/mhealth.7938>
- Jacobsen, B. (2010). Currency, Credit, Confidence and Bubbles. *Applied Economics Letters*, 17, 1653-1655. <https://doi.org/10.1080/13504850903120733>
- Jakobsson, M., & Yung, M. (1997). Applying Anti-Trust Policies to Increase Trust in a Versatile E-Money System. In *International Conference on Financial Cryptography, FC 1997: Financial Cryptography* (pp. 217-238). Berlin, Heidelberg: Springer. https://doi.org/10.1007/3-540-63594-7_80
- Jambulingam, T., Kathuria, R., & Nevin, J. R. (2011). Fairness-Trust-Loyalty Relationship under Varying Conditions of Supplier-Buyer Interdependence. *Journal of Marketing Theory and Practice*, 19, 39-56. <https://doi.org/10.2753/MTP1069-6679190103>
- Jamroga, W., Melissen, M., & Schnoor, H. (2014). On Defendability of Security Properties. *EPTCS*, 146, (2nd Workshop on Strategic Reasoning—SR14), 17-25. <https://arxiv.org/abs/1404.0836v1>
- Jayasinghe, D., Markantonakis, K., & Mayes, K. (2014). Optimistic Fair-Exchange with Anonymity for Bitcoin Users. In *Proceedings of the 11th International Conference on E-Business Engineering* (pp. 44-51). China: IEEE. <https://ieeexplore.ieee.org/document/6982058>
- Jøsang, A., Ismail, R., & Boyd, C. (2007). A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43, 618-644. <https://doi.org/10.1016/j.dss.2005.05.019>

- Leib, E. J. (2007). Friendship & the Law. *UCLA Law Review*, 54, 631-707. https://ir.lawnet.fordham.edu/faculty_scholarship/88/
- Leib, E. J. (2009). Friends as Fiduciaries. *Washington University Law Review*, 86, 665-732. <https://wustlawreview.org/wp-content/uploads/2017/09/3-18.pdf>
- Lemieux, V. L. (2016). Trusting Records: Is Blockchain Technology the Answer? *Records Management Journal*, 26, 110-139. <https://doi.org/10.1108/RMJ-12-2015-0042>
- Lemmen, C., Vos, J., & Beentjes, B. (2017). Ongoing Development of Land Administration Standards: Blockchain in Transaction Management. *European Property Law Journal*, 6, 478-502. <https://doi.org/10.1515/eplj-2017-0016>
- Leventhal, G. S. (1980). What Should Be Done with Equity Theory? New Approaches to the Study of Fairness in Social Relationships. In *Social Exchange* (pp. 27-55). Boston, MA: Springer. https://doi.org/10.1007/978-1-4613-3087-5_2
- Levin, J. (2014). *I Love the Blockchain, Just Not Bitcoin*. <https://www.coindesk.com/love-blockchain-just-bitcoin/>
- Lewicki, R. J., & Bunker, B. B. (1995). Ch. 5: Trust in Relationships: A Model of Trust Development and Decline. In *The Jossey-Bass Management Series and the Jossey-Bass Conflict Resolution Series, Conflict, Cooperation, and Justice: Essays Inspired by the Work of Morton Deutsch* (pp. 133-173). San Francisco, CA, US: Jossey-Bass.
- Lewis, D. J., & Weigert, A. (1985). Trust as a Social Reality. *Social Forces*, 63, 967-985. <https://www.jstor.org/stable/2578601>
<https://doi.org/10.1093/sf/63.4.967>
- Li, X., & Wang, C. A. (2017). The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin. *Decision Support Systems*, 95, 49-60. <https://doi.org/10.1016/j.dss.2016.12.001>
- Lieberman, J. K. (1983). *The Litigious Society*. USA: Basic Books.
- Liu, B., Yu, X. L., Chen, S., Xu, X., & Zhu, L. (2017). Blockchain Based Data Integrity Service Framework for IoT Data. In *Proceedings of the 2017 IEEE 24th International Conference on Web Services* (pp. 468-475). USA: IEEE. <https://ieeexplore.ieee.org/document/8029796>
- Liu, J., Li, W., Karame, G., & Asokan, N. (2016). Towards Fairness of Cryptocurrency Payments. Ithaca, New York: Cornell University. <https://arxiv.org/abs/1609.07256>
- Lucarelli, B. (2010). Marxian Theories of Money, Credit and Crisis. *Capital & Class*, 34, 199-214. https://www.researchgate.net/publication/247788714_Marxian_theories_of_money_credit_and_crisis
- Luhmann, N. (1979). *Trust and Power*. Chichester, Toronto: Wiley.
- Luhmann, N. (1988). Ch. 6: Familiarity, Confidence, Trust: Problems and Alternatives. In *Trust: Making and Breaking Cooperative Relations* (pp. 94-107). Great Britain: Basil Blackwell. https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf
- Luhmann, N. (1995). *Social Systems*. Stanford, CA: Stanford University Press.
- Lustig, C., & Nardi, B. (2015). Algorithmic Authority: The Case of Bitcoin. In *Proceedings of the 48th Hawaii International Conference on System Sciences* (pp. 743-752). USA: IEEE. <https://ieeexplore.ieee.org/document/7069744>
<https://doi.org/10.1109/HICSS.2015.95>
- Mann, J. R. (2000). The Role of Letters of Credit in Payment Transactions. *Michigan Law Review*, 98, 2494-2536. <https://www.jstor.org/stable/1290352>

- <https://doi.org/10.2307/1290352>
- Mansfield-Devine, S. (2017). Beyond Bitcoin: Using Blockchain Technology to Provide Assurance in the Commercial World. *Computer Fraud & Security*, 2017, 14-18. [https://doi.org/10.1016/S1361-3723\(17\)30042-8](https://doi.org/10.1016/S1361-3723(17)30042-8)
- March, J. G., & Shapira, Z. (1987). Managerial Perspectives on Risk and Risk Taking. *Management Science*, 33, 1404-1418. <http://www.jstor.org/stable/2631920>
<https://doi.org/10.1287/mnsc.33.11.1404>
- Maurer, B., Nelms, C. T., & Swartz, L. (2013). "When Perhaps the Real Problem Is Money Itself": The Practical Materiality of Bitcoin. *Social Semiotics*, 23, 261-277. <https://doi.org/10.1080/10350330.2013.777594>
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *The Academy of Management Review*, 20, 709-734. <https://www.jstor.org/stable/258792>
<https://doi.org/10.5465/amr.1995.9508080335>
- Mcallister, D. J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. *Academy of Management Journal*, 38, 24-59. <https://doi.org/10.5465/256727>
- McKnight, D. H., & Chervany, N. L. (2000). What Is Trust? A Conceptual Analysis and an Interdisciplinary Model. In *Proceedings of the AMCIS Americas Conference on Information Systems* (pp.827-833). Long Beach, California: AMCIS. <http://aisel.aisnet.org/amcis2000/382>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for E-Commerce: An Integrative Typology. *Information Systems Research*, 13, 334-359. <https://doi.org/10.1287/isre.13.3.334.81>
<https://pdfs.semanticscholar.org/b611/576195d9d883f9191b63009eb9483830a1b3.pdf>
- McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. *The Academy of Management Review*, 23, 473-490. <https://www.jstor.org/stable/259290>
<https://doi.org/10.5465/amr.1998.926622>
- Mehrling, P. (2013). Ch. 21: The Inherent Hierarchy of Money. In *Social Fairness and Economics: Economic Essays in the Spirit of Duncan Foley* (pp. 394-403). USA, Canada: Routledge.
- Menezes, A. J., Oorschot, P. C., & Vanstone, S. A. (1996). *Handbook of Applied Cryptography*. New York: CRC Press. <https://doi.org/10.1201/9781439821916>
<http://math.fau.edu/bkhadka/Syllabi/A%20handbook%20of%20applied%20cryptograpy.pdf>
- Mertz, D. (2001). *Introduction to Cryptology, Part 1, Basic Cryptology Concepts*. IBM. <https://www.ibm.com/developerworks/tivoli/tutorials/s-crypto/s-crypto.html>
- Meyer, C., & Hudon, M. (2018). Money and the Commons: An Investigation of Complementary Currencies and Their Ethical Implications. *Journal of Business Ethics*, 2018, 1-16. <https://doi.org/10.1007/s10551-018-3923-1>
- Michaels, D. (2017). *App Maker Halts \$15 Million Initial Coin Offering after SEC Investigation*. The Wall Street Journal. <https://www.wsj.com/articles/app-maker-halts-15-million-initial-coin-offering-after-se-c-investigation-1513012449>
- Mishra, A. K. (1996). Ch. 13: Organizational Responses to Crisis: The Centrality of Trust. In *Trust in Organizations: Frontiers of Theory and Research* (pp. 261-287), USA: SAGE. <https://doi.org/10.4135/9781452243610.n13>

- Monetary Authority of Singapore (2017). *MAS Clarifies Regulatory Position on the Offer of Digital Tokens in Singapore*. Singapore Government.
<http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx>
- Morse, A. E. (2018). From Rai Stones to Blockchains: The Transformation of Payments. *Computer Law & Security Review*, 34, 946-953.
<https://doi.org/10.1016/j.clsr.2018.05.035>
- Mosier, K. L., & Skitka, L. J. (1996). Ch. 10: Human Decision Makers and Automated Decision Aids: Made for Each Other? In *Automation and Human Performance: Theory and Applications* (pp. 201-220). New York: Routledge.
- Muir, B. M., & Moray, N. (1996). Trust in Automation, Part II, Experimental Studies of Trust and Human Intervention in a Process Control Simulation. *Ergonomics*, 39, 429-460.
<https://www.ncbi.nlm.nih.gov/pubmed/8849495>
<https://doi.org/10.1080/00140139608964474>
- Muzammal, M., Qu, Q., & Nasrulin, B. (2019). Renovating Blockchain with Distributed Databases: An Open Source System. *Future Generation Computer Systems*, 90, 105-117.
<https://doi.org/10.1016/j.future.2018.07.042>
- Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.
<https://bitcoin.org/bitcoin.pdf>
- NASAA (2018). *NASAA Reminds Investors to Approach Cryptocurrencies, Initial Coin Offerings and Other Cryptocurrency-Related Investment Products with Caution*. Washington, DC: North American Securities Administrators Association.
<http://www.nasaa.org/44073/nasaa-reminds-investors-approach-cryptocurrencies-initial-coin-offerings-cryptocurrency-related-investment-products-caution/>
- Nathan, S. B. (2003). Letter of Credit Issuer Not Entitled to Payment of Surplus Funds Drawn by Beneficiary. *Business Credit*, 105, 33-37.
- Newby, E. (2007). *The Suspension of Cash Payments as a Monetary Regime*. Centre for Dynamic Macroeconomic Analysis Working Paper Series (CDMA07/07).
<https://doi.org/10.2139/ssrn.961799>
<https://www.st-andrews.ac.uk/cdma/papers/wp0707.pdf>
- Nguyen, Q. K. (2016). Blockchain—A Financial Technology for Future Sustainable Development. In *Proceedings of the 3rd International Conference on Green Technology and Sustainable Development* (pp. 51-54). Taiwan: IEEE.
<https://ieeexplore.ieee.org/document/7796617>
- Novak, M. (2018). *Crypto-Altruism: Some Institutional Economic Considerations*. SSRN.
<https://doi.org/10.2139/ssrn.3230541>
- Nyman, C. (2003). The Social Nature of Money: Meanings of Money in Swedish Families. *Women's Studies International Forum*, 26, 79-94.
[https://doi.org/10.1016/S0277-5395\(02\)00357-6](https://doi.org/10.1016/S0277-5395(02)00357-6)
- Oliver, R. L. (1999). Whence Consumer Loyalty? *Journal of Marketing*, 63, 33-44.
<https://www.jstor.org/stable/1252099>
- Ølnes, S., Ubacht, J., & Janssen, M. (2017). Blockchain in Government: Benefits and Implications of Distributed Ledger Technology for Information Sharing. *Government Information Quarterly*, 34, 355-364. <https://doi.org/10.1016/j.giq.2017.09.007>
- Orcutt, M. (2015). *Why Bitcoin Could Be Much More Than a Currency*. MIT Technology Review.
<https://www.technologyreview.com/s/537246/why-bitcoin-could-be-much-more-than-a-currency/>

- Otte, P., Vos, M., & Pouwelse, J. (2017). TrustChain: A Sybil-Resistant Scalable Blockchain. *Future Generation Computer Systems*, 2017, 1-11.
<https://doi.org/10.1016/j.future.2017.08.048>
- Oxford Dictionary (2018). *Oxford University Press*.
<https://en.oxforddictionaries.com/definition/token>
- Özkan, Ö., Özçelik, O., & Kılıç, S. (2016). Important and Critical Issues of Complying Presentation Based Upon Letter of Credit (L/C) Payment. *Journal of International Trade, Logistics and Law*, 2, 73-80.
- Paech, P. (2011). *Cross-Border Issues of Securities Law: European Efforts to Support Securities Markets with a Coherent Legal Framework*. Brussels, Belgium: Directorate General for Internal Policies, Policy Department A: Economic and Scientific Policy, Economic and Monetary Affairs, The European Parliament.
<http://www.europarl.europa.eu/document/activities/cont/201106/20110606ATT20781/20110606ATT20781EN.pdf>
- Pagden, A. (1988). Ch. 8: The Destruction of Trust and its Economic Consequences in the Case of Eighteenth-Century Naples. In *Trust: Making and Breaking Cooperative Relations* (pp. 127-141). Great Britain: Basil Blackwell.
https://www.nuffield.ox.ac.uk/users/gambetta/Trust_making%20and%20breaking%20cooperative%20relations.pdf
- Pangas, S. H., & Park, A. (2017). The Newest Regulatory Enigma: Bitcoins and Other Virtual Currencies. *The Investment Lawyer*, 24, 15-22.
https://www.martindale.com/legal-news/article_eversheds-sutherland-us-llp_2502237.htm
- Peck, M. (2016). A Blockchain Currency that Beats Bitcoin on Privacy. *IEEE Spectrum*, 53, 11-13.
<https://spectrum.ieee.org/computing/networks/a-blockchain-currency-that-beats-bitcoin-on-privacy>
- Peck, M. (2017). Blockchains: How They Work and Why They'll Change the World. *IEEE Spectrum*, 54, 26-35. <https://ieeexplore.ieee.org/document/8048836>
<https://doi.org/10.1109/MSPEC.2017.8048836>
- Perez, Y. B. (2015). *8 Banking Giants Embracing Bitcoin and Blockchain Tech*. *CoinDesk*.
<https://www.coindesk.com/8-banking-giants-bitcoin-blockchain/>
- Peters, G., Panayi, E., & Chapelle, A. (2015). *Trends in Crypto-Currencies and Blockchain Technologies: A Monetary Theory and Regulation Perspective*.
<https://arxiv.org/abs/1508.04364>
- Pettit, P. (1995). The Cunning of Trust. *Philosophy and Public Affairs*, 24, 202-225.
<http://www.jstor.org/stable/2961900>
<https://doi.org/10.1111/j.1088-4963.1995.tb00029.x>
- PEW Research Center (1997). *Trust and Citizen Engagement in Metropolitan Philadelphia: A Case Study*.
<http://www.people-press.org/1997/04/18/trust-and-citizen-engagement-in-metropolitan-philadelphia-a-case-study/>
- Phillips, D. (1998). Ch. 9: Cryptography, Secrets, and the Structuring of Trust. *Technology and Privacy: The New Landscape* (pp. 243-276). Cambridge, MA: The MIT Press.
- Pieters, W. (2011). Explanation and Trust: What to Tell the User in Security and AI? *Ethics and Information Technology*, 13, 53-64.
<https://doi.org/10.1007/s10676-010-9253-3>
- Popper, N. (2017). *Initial Coin Offerings Horrify a Former S.E.C. Regulator*. The New

- York Times.
<https://www.nytimes.com/2017/11/26/business/initial-coin-offering-critic.html>
- Porter, L. W., Lawler, E. E., & Hackman, J. R. (1974). *Behavior in Organizations*. New York: McGraw-Hill.
- Post, J. (2011). Governance, Accountability, and Trust: A comment on the Work of Tamar Frankel. *Boston University Law Review*, 91, 1165-1173.
<http://www.bu.edu/law/journals-archive/bulr/documents/post.pdf>
- Puthal, D., Malik, N. Mohanty, S., Kougianos, E., & Yang, C. (2018). The Blockchain as a Decentralized Security Framework. *IEEE Consumer Electronics Magazine*, 7, 18-21.
<https://ieeexplore.ieee.org/document/8287055>
<https://doi.org/10.1109/MCE.2017.2776459>
- Qian, X., Zhang, G., & Cao, T. (2018). Money Following Trust: Evidence from China's High-Value Payment System. *International Review of Finance*, 2018, 1-28.
<https://onlinelibrary.wiley.com/doi/epdf/10.1111/irfi.12184>
<https://doi.org/10.1111/irfi.12184>
- Radojičić, J., & Radovanović, P. (2015). Narrow Banking—Banking System without Private Issuance of Credit Money as a Solution for More Resistant Banks and More Stable Financial System. *Economic Themes*, 53, 375-396.
<https://doi.org/10.1515/ethemes-2015-0022>
- Ramey, C. (2018). The Crypto Crime Wave Is Here. *The Wall Street Journal*.
<https://www.wsj.com/articles/the-crypto-crime-wave-is-here-1524753366?mod=searchresults&page=1&pos=2>
- Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in Close Relationships. *Journal of Personality and Social Psychology*, 49, 95-112.
<https://doi.org/10.1037/0022-3514.49.1.95>
- Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2000). Reputation Systems. *Communications of the ACM*, 43, 45-48. <https://dl.acm.org/citation.cfm?id=355122>
<https://doi.org/10.1145/355112.355122>
- Rethink Music (2015). *Rethink Music: Transparency and Money Flows in the Music Industry—Recommendations to Increase Transparency, Reduce Friction, and Promote Fairness in the Music Industry*. Boston, Massachusetts, USA: Berklee Institute of Creative Entrepreneurship.
<https://www.berklee.edu/sites/default/files/Fair%20Music%20-%20Transparency%20and%20Payment%20Flows%20in%20the%20Music%20Industry.pdf>
- Reuten, G. (1988). The Money Expression of Value and the Credit System: A Value-Form Theoretic Outline. *Capital & Class*, 12, 121-141.
<https://doi.org/10.1177/030981688803500108>
- Risius, M., & Spohrer, K. (2017). A Blockchain Research Framework: What We (Don't) Know, Where We Go from Here, and How We Will Get There. *Business & Information Systems Engineering*, 59, 385-409.
https://www.researchgate.net/publication/321539709_A_Blockchain_Research_Framework_What_We_don't_Know_Where_We_Go_from_Here_and_How_We_Will_Get_There <https://doi.org/10.1007/s12599-017-0506-0>
- Roettgers, J. (2018). Block Chain Mania. *Variety*, 339, 42-45.
<https://search.proquest.com/docview/2025763667/fulltext/3F37CFF8EE044BB7PQ/1?accountid=14615>
- Rosdolsky, R. (1977). *The Making of Marx's Capital*. London, UK: Pluto Press.
http://ouleft.org/wp-content/uploads/rosdolsky-the-making-of-marxs-capital_cs.pdf
- Roth-Berghofer, T. R., & Cassens, J. (2005). Mapping Goals and Kinds of Explanations to

- the Knowledge Containers of Case-Based Reasoning Systems. In *Case-Based Reasoning Research and Development, Lecture Notes in Computer Science*, 3620 (pp. 451-464). Germany: Springer-Verlag Berlin Heidelberg. https://doi.org/10.1007/11536406_35
- Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Introduction to Special Topic Forum, Not So Different After All: A Cross-Discipline View of Trust. *Academy of Management Review*, 23, 393-404. <https://doi.org/10.5465/amr.1998.926617>
<https://journals.aom.org/doi/10.5465/amr.1998.926617>
- Rowe, S. (2017). Blockchain Technology Fosters Its Own Concerns: The Financial Transaction Security Technology Leaves Many Companies Worried. *Customer Relationship Management Magazine*, 21, 19. <https://www.destinationcrm.com/Articles/ReadArticle.aspx?ArticleID=120793>
- Ruwitch, J., & Kelly, J. (2017). *China Hits Booming Cryptocurrency Market with Coin Fundraising Ban*. Reuters. <https://www.reuters.com/article/us-china-finance-digital/china-hits-booming-cryptocurrency-market-with-coin-fundraising-ban-idUSKCN1BF0R7>
- Ryan, H. R. (1983). Letters of Credit Supporting Debt for Borrowed Money: The Standby as Backup. *Banking Law Journal*, 100, 404-422. <https://heinonline.org/HOL/P?h=hein.journals/blj100&i=428>
- Sargent, T., & Velde, F. (1999). The Big Problem of Small Change. *Journal of Money, Credit and Banking*, 31, 137-161. <https://www.jstor.org/stable/2601227>
<https://doi.org/10.2307/2601227>
- Sas, C., & Khairuddin, I. E. (2017). Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users. In *Proceedings of the CHI'17 ACM Conference Computer Human Interaction 2017* (pp. 6499-6510). New York: ACM Press. <https://dl.acm.org/citation.cfm?id=3025886>
- Savelyev, A. (2018). Some Risks of Tokenization and Blockchainization of Private Law. *Computer Law & Security Review*, 34, 863-869. <https://doi.org/10.1016/j.clsr.2018.05.010>
- Schelling, T. C. (1965). Strategic Analysis and Social Problems. *Social Problems*, 12, 367-379. <https://www.jstor.org/stable/798837>
<https://doi.org/10.2307/798837>
- Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W.W. Norton & Company.
- Schwienbacher, A., & Larralde, B. (2012). Part IV; Ch. 12: Crowdfunding of Entrepreneurial Ventures. In *The Oxford Handbook of Entrepreneurial Finance* (pp. 369-391). New York: Oxford University Press.
- Securities and Exchange Commission (2017a). *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO (Securities Exchange Act Of 1934, Release No. 81207)*. USA: U.S. Securities and Exchange Commission. <https://www.sec.gov/litigation/investreport/34-81207.pdf>
- Securities and Exchange Commission (2017b). *Investor Alerts and Bulletins, Investor Bulletin: Initial Coin Offerings*. USA: U.S. Securities and Exchange Commission. https://www.sec.gov/oiea/investor-alerts-and-bulletins/ib_coinofferings
- Securities and Exchange Commission (2017c). *SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors*. USA: U.S. Securities and Exchange Commission. <https://www.sec.gov/news/press-release/2017-176>
- Securities and Exchange Commission (2017d). *SEC Emergency Action Halts ICO Scam*. Washington, D.C.: U.S. Securities and Exchange Commission.

- <https://www.sec.gov/news/press-release/2017-219>
- Seele, P. (2018). Let Us Not Forget: Crypto Means Secret. Cryptocurrencies as Enabler of Unethical and Illegal Business and the Question of Regulation. *Humanist Management Journal*, 3, 133-139. <https://doi.org/10.1007/s41463-018-0038-x>
- Shackelford, S. J., & Myers, S. (2017). Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace. *The Yale Journal of Law and Technology*, 19, 334-388. https://www.yjolt.org/sites/default/files/shackelford19yjolt334_0.pdf
- Shiho, K. (2018). Blockchain for a Trust Network among Intelligent Vehicles. *Advances in Computers*, 111, 43-68. <https://doi.org/10.1016/bs.adcom.2018.03.010>
- Shin, H. (2015). Paper Money, the Nation, and the Suspension of Cash Payments in 1797. *The Historical Journal*, 58, 415-442. <https://doi.org/10.1017/S0018246X14000284>
- Simiand, F. (1934). La Monnaie Réalité Sociale. *Annales Sociologiques, Série D, Sociologie Économique, Fasc. 1*, 1-58. <https://www.jstor.org/stable/27882162>
- Simmel, G. (1950). *The Sociology of Georg Simmel* (Translated & Edited by Kurt H. Wolff). Glencoe, Illinois: The Free Press. <https://archive.org/details/sociologyofgeorg030082mbp/page/n21>
- Sitkin, S. B., & Pablo, A. L. (1992). Reconceptualizing the Determinants of Risk Behavior. *The Academy of Management Review*, 17, 9-38. <https://www.jstor.org/stable/258646> <https://doi.org/10.5465/amr.1992.4279564>
- Sitkin, S. B., & Roth, N. L. (1993). Explaining the Limited Effectiveness of Legalistic “Remedies” for Trust/Distrust. *Organization Science*, 4, 367-392. <https://www.jstor.org/stable/2634950> <https://doi.org/10.1287/orsc.4.3.367>
- Six, F., & Sorge, A. (2008). Creating a High-Trust Organization: An Exploration into Organizational Policies that Stimulate Interpersonal Trust Building. *Journal of Management Studies*, 45, 857-884. <https://doi.org/10.1111/j.1467-6486.2007.00763.x>
- Smolenski, N. (2018). The Evolution of Trust: The Ultimate Social Impact of Blockchain Technology Depends on Who Controls Our Digital Identities. *Scientific American*, 318, 38-41. <https://doi.org/10.1038/scientificamerican0118-38> <https://www.scientificamerican.com/article/the-evolution-of-trust-in-a-digital-economy/>
- Sørmo, F., Cassens, J., & Aamodt, A. (2005). Explanation in Case-Based Reasoning-Perspectives and Goals. *Artificial Intelligence Review*, 24, 109-143. <https://doi.org/10.1007/s10462-005-4607-7>
- Stein, J. (2009). An Update on the Bankruptcy Law of Large Letters of Credit for Leases. *Real Property, Trust and Estate Law Journal*, 44, 299-321. https://www.joshuastein.com/PDF/An_Update_Bankruptcy_Large_Letters_of_Credit_for_Leases_145_264.pdf
- Sur, S. (2011). Loyalty Relationships in Technology-Based Remote Service Encounters. *Journal of Services Research*, 11, 121-134. <http://search.ebscohost.com/login.aspx?direct=true&db=bsh&AN=70139478&site=ehost-live>
- Swift, A., & Ander, S. (2016). *Americans Using Cash Less Compared with Five Years Ago*. Gallup. <https://news.gallup.com/poll/193649/americans-using-cash-less-compared-five-years-ago.aspx>
- Telpner, J. S., & Ahmadifar, T.M. (2017). ICOs: The DAO, and the Investment Company

- Act of 1940. *The Investment Lawyer*, 24, 16-33.
<https://www.sandw.com/assets/htmldocuments/ICOs%20The%20DAO%20and%20the%20Investment%20Company%20Act.pdf>
- Texas State Securities Board (2018). *Emergency Cease and Desist Order (No. ENF-18-CDO-1754)*. Austin, Texas: Texas State Securities Board.
https://www.ssb.texas.gov/sites/default/files/BitConnect_ENF-18-CDO-1754.pdf
- Thompson, C. (2018). In Bitcoin We Trust: What Benjamin Franklin and Jefferson Davis Can Teach Today's Cryptocurrency Creators. *Smithsonian*, 49, 13-90.
<https://www.ccpl.org/eds/detail?db=edsgwh&an=edsgcl.536388568&isbn=edsgwh>
- Thrift, N. (2005). *Knowing Capitalism*. London, California, India: SAGE Publications.
- Tian, Q., & Sanchez, J. I. (2017). Does Paternalistic Leadership Promote Innovative Behavior? The Interaction between Authoritarianism and Benevolence. *Journal of Applied Social Psychology*, 47, 235-246. <https://doi.org/10.1111/jasp.12431>
- Truong, N., Um, T.-W., Zhou, B., & Lee, G. M. (2018). Strengthening the Blockchain-Based Internet of Value with Trust. In *Proceedings of the IEEE International Conference on Communications* (pp. 1-7). USA: IEEE.
<https://ieeexplore.ieee.org/abstract/document/8423014>
- Tseng, L. (2017). Bitcoin's Consistency Property. In *Proceedings of the 2017 IEEE 22nd Pacific Rim International Symposium on Dependable Computing* (pp. 219-220). New Zealand: IEEE. <https://ieeexplore.ieee.org/document/7920619>
<https://doi.org/10.1109/PRDC.2017.39>
- Tyler, T. R., & DeGoey, P. (1996). Ch. 16: Trust in Organizational Authorities: The Influence of Motive Attributions on Willingness to Accept Decisions. In *Trust in Organizations: Frontiers of Theory and Research* (pp. 331-356). USA: SAGE.
<https://doi.org/10.4135/9781452243610.n16>
- UK Consumer Credit Act (1974). *Section 14*.
<https://www.legislation.gov.uk/ukpga/1974/39/section/14>
- Umeh, J. (2016). Blockchain Double Bubble or Double Trouble? *ITNOW*, 58, 58-61.
<https://doi.org/10.1093/itnow/bww026>
- Uslaner, E. M. (2002). Ch. 1: Trust and the Good Life. In *The Moral Foundations of Trust* (pp. 1-13). Cambridge, UK: Cambridge University Press.
<http://catdir.loc.gov/catdir/samples/cam031/2001052721.pdf>
- Uzzi, B. (1997). Social Structure and Competition in Interfirm Networks: The Paradox of Embeddedness. *Administrative Science Quarterly*, 42, 35-67.
<https://doi.org/10.2307/2393808>
<https://www.jstor.org/stable/2393808>
- Vasilomanolakis, E., Wolf, J. H., Böck, L., Karuppayah, S., & Mühlhäuser, M. (2017). *I Trust my Zombies: A Trust-enabled Botnet*. Ithaca, New York: Cornell University.
<https://arxiv.org/abs/1712.03713>
- Veuger, J. (2018). Trust in a Viable Real Estate Economy with Disruption and Blockchain, *Facilities*, 36, 103-120. <https://doi.org/10.1108/F-11-2017-0106>
- Walton, R. (2006). Cryptography and Trust. *Information Security Technical Report*, 11, 68-71. <https://doi.org/10.1016/j.istr.2006.03.002>
- Webb, A. (2015). 8 Tech Trends to Watch in 2016. *Harvard Business Review*.
<https://hbr.org/2015/12/8-tech-trends-to-watch-in-2016>
- Weinstock, D. M. (1999). Building Trust in Divided Societies. *The Journal of Political Philosophy*, 7, 287-307. <https://doi.org/10.1111/1467-9760.00078>
<https://onlinelibrary.wiley.com/doi/pdf/10.1111/1467-9760.00078>

- Williamson, S. (2018). Is Bitcoin a Waste of Resources? *Federal Reserve Bank of St. Louis Review*, 100, 107-115. <https://doi.org/10.20955/r.2018.107-15>
- World Economic Forum (2016). *The Future of Financial Infrastructure: An Ambitious Look at How Blockchain Can Reshape Financial Services*. http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf
- Wu, C.-C., Huang, Y., & Hsu, C.-L. (2014). Benevolence Trust: A Key Determinant of User Continuance Use of Online Social Networks. *Information Systems and E-Business Management*, 12, 189-211. <https://doi.org/10.1007/s10257-013-0216-1>
- Xu, L. D., Xu, E. L., & Li, L. (2018). Industry 4.0: State of the Art and Future Trends. *International Journal of Production Research*, 56, 2941-2962. <https://doi.org/10.1080/00207543.2018.1444806>
- Xu, L., Shah, N., Chen, L., Diallo, N., Gao, Z., Lu, Y., et al. (2017). Enabling the Sharing Economy: Privacy Respecting Contract Based on Public Blockchain. In *BCC'17 Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts* (pp. 15-21). United Arab Emirates: ACM. <https://doi.org/10.1145/3055518.3055527>
- Yin, W., Wen, Q., Li, W., Zhang, H., & Jin, Z. P. (2018). An Anti-Quantum Transaction Authentication Approach in Blockchain. *IEEE Access*, 6, 5393-5401. <https://ieeexplore.ieee.org/document/8242360>
<https://doi.org/10.1109/ACCESS.2017.2788411>
- Yli-Huomo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. *PLoS ONE*, 11, 1-27. <http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0163477&type=printable> <https://doi.org/10.1371/journal.pone.0163477>
- You, J. S. (2012). Social Trust: Fairness Matters More Than Homogeneity. *Political Psychology*, 33, 701-721. <https://doi.org/10.1111/j.1467-9221.2012.00893.x>
- Zak, P. J., & Knack, S. (2001). Trust and Growth. *The Economic Journal*, 111, 295-321. <http://www.sba.muohio.edu/davisgk/growth%20readings/19.pdf>
<https://doi.org/10.1111/1468-0297.00609>
- Zelizer, V. (1989). The Social Meaning of Money: “Special Monies”. *American Journal of Sociology*, 95, 342-377. <https://www.jstor.org/stable/2780903>
<https://doi.org/10.1086/229272>
- Zetzsche, D. A., Buckley, R. P., Arner, D. W., & Föhr, L. (2018). *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators*. University of Luxembourg Law Working Paper, No. 11/2017, UNSW Law Research Paper, No. 17-83, University of Hong Kong Faculty of Law Research Paper, No. 2017/035, European Banking Institute Working Paper Series, 18/2018. <https://ssrn.com/abstract=3072298>
- Zhang, R., & Preneel, B. (2017). Publish or Perish: A Backward-Compatible Defense Against Selfish Mining in Bitcoin. In *Topics in Cryptology—CT-RSA 2017, CT-RSA 2017, Lecture Notes in Computer Science, 10159* (pp. 277-292). Cham: Springer. https://doi.org/10.1007/978-3-319-52153-4_16
- Zikratov, I., Kuzmin, A., Akimenko, V., Niculichev, V., & Yalansky, L. (2017). Ensuring Data Integrity Using Blockchain Technology. In *Proceedings of the 20th Conference of Open Innovations Association* (pp. 534-539). Russia: IEEE. <https://ieeexplore.ieee.org/document/8071359>
- Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *IEEE Security and Privacy Workshops* (pp. 180-184). San Jose, CA, USA: IEEE. <https://ieeexplore.ieee.org/document/7163223>
<https://doi.org/10.1109/SPW.2015.27>