frontiers in Blockchain

PERSPECTIVE
published: 15 November 2019
doi: 10.3389/fbloc.2019.00020

The Middleman Is Dead, Long Live the Middleman: The "Trust Factor" and the Psycho-Social Implications of Blockchain

Andrea Gaggioli[1,2]*, *Shayan Eskandari*[3], *Pietro Cipresso*[1,2] and *Edoardo Lozza*[1]

[1] Department of Psychology, Universitá Cattolica del Sacro Cuore, Milan, Italy, [2] Applied Technology for Neuro-Psychology Lab, IRCCS Istituto Auxologico Italiano, Milan, Italy, [3] Gina Cody School of Engineering and Computer Science, Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada

Blockchain is widely regarded as a breakthrough innovation that may have a profound impact on the economy and society, of a magnitude comparable to the effects of the introduction of the Internet itself. In essence, a blockchain is a decentralized peer-to-peer network with no central authority figure, which adds information to the distributed database by collectively validating the accuracy of data. Since each node of the network participates in the review and confirmation of the new information before being accepted, the need for a trustworthy intermediary is eliminated. However, as trust plays an essential role in affecting decisions when transacting with one another, it is important to understand which implications the decentralized nature of blockchain may have on individuals' sense of trust. In this contribution, we argue that the adoption of blockchain is not only a technological, but foremostly a psychological challenge, which crucially depends on the possibility of creating a trust management approach that matches the underlying distributed communication system. We first describe the decentralization technologies and possibilities they hold for the near future. Next, we discuss the psycho-social implications of the introduction of decentralized processes of trust, examining some potential scenarios, and outline a research agenda.

Keywords: trust, blockchain, smart contract, psychology, user experience

OPEN ACCESS

Edited by:
Panos Kourouthanassis, Ionian University, Greece

Reviewed by:
George Theocharides, Cyprus International Institute of Management, Cyprus
Ioannis Vlachos, National Technical University of Athens, Greece

***Correspondence:**
Andrea Gaggioli
andrea.gaggioli@unicatt.it

Specialty section:
This article was submitted to Blockchain Technologies, a section of the journal Frontiers in Blockchain

Received: *09 May 2019*
Accepted: *30 October 2019*
Published: *15 November 2019*

Citation:
Gaggioli A, Eskandari S, Cipresso P and Lozza E (2019) The Middleman Is Dead, Long Live the Middleman: The "Trust Factor" and the Psycho-Social Implications of Blockchain. Front. Blockchain 2:20. doi: 10.3389/fbloc.2019.00020

INTRODUCTION AND MOTIVATION

The blockchain phenomena started within a cryptography mailing list known as *Cypherpunks* (Assange et al., 2016). A paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" written by an anonymous author named Satoshi Nakamoto surfaced on October 31, 2008. The premise of the paper was to have a system for electronic transactions without relying on third-party trust (Nakamoto, 2008). In blockchain, there is no central server or central point of control. All users of the blockchain run a software (node) to connect to the peer-to-peer network. All nodes have equal access and control, and they all should agree on the final state of the blockchain based on the defined set of rules known as the consensus protocol. Bitcoin, the first and one of simplest blockchain applications, is technically a decentralized ledger (database), where all the nodes have a fully verifiable copy of the ledger. Nodes can use their processing power to verify recent transactions and append them as batches, called blocks, to the blockchain. They do so by solving complex

mathematical equations and broadcast the solution to the network once found. All other nodes verify the solution, and the first verified answer adds its block to the blockchain and receives newly minted Bitcoins as a reward from the protocol (**Figure 1**).

An important implication of blockchain's decentralized approach concerns identity management. With the rise of the Internet, the concept of username and password was introduced as the authentication method for users in websites and services. The identity of each individual within a service is saved on the website's database and can be modified by website administrators at will. In contrast, in blockchain the identity of an individual or an entity boils down to a pair of cryptographic keys, a public key used as the address (name, public identity) and a private key used to prove the ownership of the identity, which should remain confidential. The "user" is fully responsible for the security and proper backup of the private key. Only the public identity of the user is saved on the service provider's end and only the user could prove their identity using their private key signature. Crucially, private key cannot be recovered if lost, and if it is leaked, anyone could impersonate or steal the digital asset controlled by that private key.

The choice of using keys instead of passwords is still specific to tech-savy users, and regular Internet users do not seem to be ready for such a change (Eskandari, 2015). Actually, for better user experience, it is common for users to trade off security for usability. The service provider could keep the keys and the user could use a traditional username and password authentication method to login; however, in this scenario, it would be difficult to distinguish such system from current central technologies where the service provider is in full control of the users' assets. Another fundamental difference between blockchain applications and current technologies is with whom users associate the application. There is no main or central entity to think about and address in blockchain applications, unlike other technologies commonly run by a company or a consortium to address. When having an issue with the system, no one entity is responsible, but the collective network of developers and people should be notified. Their effort to fix the issue depends on the severity or means of the report, not to mention the consensus required to deploy the changes within the network (De Filippi and Loveluck, 2016).

Blockchain networks are broadly classified in two main categories, namely *permissionless* and *permissioned* (Wüst and Gervais, 2018). Permissionless (or public) blockchains are defined as such because they don't require an authorization for accessing the network, execute transactions or partake to the verification and creation of a new block. Bitcoin and Ethereum are the most popular examples of permissionless networks, which are characterized by a fully decentralized structure, whose access authorizations are shared among all nodes of the network. In permissionless blockchains, no network user has more privileges than others; furthermore, no one can control, modify or eliminate other's information which are stored in the network, or altering its functioning protocol. Permissioned networks (also known as "consortium blockchain" or "private blockchain"), on the other hand, can be owned by one or more entities and users' identities can be known. They are subject to a central authority, which defines who can access the network and which roles the user can have, also defining rules about the accessibility of registered data. Thus, in these kinds of networks, only a selected and trusted set of nodes are allowed to partake in the verification of the transactions. An example of this type of blockchain network is Hyperledger by IBM, which is an open-source collaborative project of blockchains and other similar tools. That said, public blockchains software are open source and can be used in a different setup as a private blockchain (e.g., Ethereum Proof of Authority), the difference being in the details of how users can engage with the protocol and if there are users with more control than the others.

Because of its decentralized network structure that disintermediates trusted third parties, blockchain has allegedly been regarded as a "trust-free technology" (Beck et al., 2016). However, there is currently little consensus as to whether or not this claim is valid, since, as it will be shown later, trust is an elusive and multifaceted concept. Would users really accept a shift in trust from people and legal systems to technology? In what follows, we argue that in order to address this question, it is important to focus not only on the technical, but also on the psycho-social factors that shape a "distributed trust" system. We start from a brief review of literature on trust (section Defining Trust), then we discuss and compare psycho-social issues of trust in blockchain and other information systems (section Trust in ICTs and Blockchain); finally, we sketch what we consider as the most relevant challenges for psycho-social research in this field (section A Research Agenda for Studying the Psychosocial Implications of Trust in Blockchain).

DEFINING TRUST

Trust is a key element that mediates the interaction between human (and non-human) agents, which is commonly regarded as a fundamental enabler of network relations (Jarillo, 1988; Newell and Swan, 2000) and a driver of social capital (Coleman, 1990; Fukuyama, 1995). Although trust is one of the most-referenced constructs in the social sciences, no generally-accepted agreement exists on its definition, which depends on the actors, relationships, behaviors, and contexts that are considered (Castaldo et al., 2010). Despite this heterogeneity, scholars tend to converge on at least some essential dimensions of trust (Rousseau et al., 1998), which are summarized in Mayer et al. (1995) frequently-cited definition as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor" (p. 712). This definition suggests that vulnerability is a core aspect for trust to occur, and that the lower is the degree of trust, the lower is the risk-taking behavior, which means lower involvement by the trustor in an activity characterized by higher perceived risk. Mayer et al. proposes that trust is characterized by three key antecedents, which are the ability, benevolence, and integrity of the trustee. Ability refers to the capability of the trustee to fulfill a task or an obligation, address a request, or provide a competent answer. Benevolence is the extent to which a trustee is believed to care about the trustor,

aside from an egocentric profit motive; also, benevolence suggests that the trustee has some specific attachment to the trustor. The third determinant of trust is integrity, which is described by Mayer et al. as the trustor's perception that the trustee adheres to a set of principles that the trustor finds acceptable, i.e., loyalty, honesty, correctness.

Individual vs. Interpersonal Trust

A further useful distinction is between individual and interpersonal trust. Individual (or dispositional) trust concerns how personality characteristics influence the process of making a trust-related decision. In contrast, interpersonal trust refers to the social dimension of this process and focuses on the factors that affect trust relationships among people. Interpersonal trust has received much more attention in the psychological literature, given the central role that this aspect has in shaping relationships across the life-course of the individual (Erikson, 1963; Bowlby, 1969; Deutsch, 1973). Rotter (1967) defined interpersonal trust as "an expectancy held by an individual or group that the word, promise, or written statement of another individual or group can be relied upon" (p. 651). Three broad perspectives on trust can be identified. The behavioral perspective sees trust as a reciprocal relationship, which facilitates cooperation through the observable choices that are performed by an actor in an interpersonal context (Lewicki et al., 2006). The cognitive perspective grounds trust on evidence of trustworthiness and available knowledge, i.e., "the extent to which a person is confident in, and willing to act on the basis of, the words, actions, and decisions of another" (McAllister, 1995, p. 25). Finally, the affective view focuses on the role that emotions play in shaping trust, i.e., how they influence perceptions of trustworthiness, judgments and the extent of risk taking (Dunn and Schweitzer, 2005). Thielmann and Hilbig (2015) defined interpersonal trust as "a risky choice of making oneself dependent on the actions of another in a situation of uncertainty, based upon some expectation of whether the other will act in a benevolent fashion despite an opportunity to betray." (p. 251). This definition highlights three key features of trusting: first, trust is associated with a risk and an uncertain outcome; second, trust involves vulnerability; third, trust is based on the expectation that the trusted party will reciprocate the initial trust act. This conceptualization also separates the cognitive and the behavioral component of trust, by differentiating between expectation (i.e., cognition) and risky dependence choice (i.e., behavior). According to Thielmann and Hilbig's model, an individual's decision to trust results by the interplay of three determinants, which are: (i) attitudes toward risky prospects (i.e., risk aversion and loss aversion), (ii) betrayal sensitivity (based on trust cues, prior trust experiences, and/or social projection), and (iii) trustworthiness expectations. Noteworthily, the authors suggest that these components of trust are linked to individual differences and personality traits. Specifically, from their summary of the literature they conclude that the first component (attitudes toward risky prospects) is influenced by an individual's trait anxiety and fear; betrayal sensitivity is affected by the trait forgiveness; and trustworthiness expectations are influenced by the personality trait social projection, which reflects an individual's own trustworthiness (i.e., fairness and honesty) as projected onto another. In summary, this brief overview of definitions of trust found in the psycho-social literature suggests that trust is a multifaceted process, which entails dimensions of risk, vulnerability, and expectations/beliefs: also, trust is not immune from the personal characteristics of the trustor, as individual traits and life experiences can play a significant role in shaping the decision to trust.

TRUST IN ICTS AND BLOCKCHAIN

Trust is commonly regarded as a key driver of user's adoption of ICTs. In this context, trust can be defined as the willingness to depend on and be vulnerable to an information system in uncertain and risky environments (Gefen et al., 2008; Thielsch et al., 2018). For example, at the turn of the century, the development of e-commerce raised a challenge similar to the one that blockchain is facing nowadays: online businesses needed to create adequate initial trust in order to convince consumers to adopt e-commerce sites. To address this issue, different frameworks and models were developed to help the design of e-commerce systems that support customers' trust (Gefen, 2002; Gefen et al., 2003, 2008; McKnight et al., 2004; Wang and Emurian, 2005; Beldad et al., 2010; Hong and Cha, 2013). In contrast, comparatively little research has examined trust in the blockchain context (Hawlitschek et al., 2018) and in particular within the psychological literature, where the topic is almost inexistent. Yet, as it will be discussed below, the introduction of blockchain may impact trust in fundamental ways, as machines will be tasked with ensuring it while supposedly diminishing or eliminating the need for human intermediates' (i.e., central authorities) control.

How Blockchain Affects the Notion of Trust

As a first example, we can compare a blockchain application (e.g., Bitcoin) to a centralized money transfer service (e.g., Paypal). If Alice sends money to Bob using Paypal, both parties of the transaction should trust Paypal to intermediate this transaction and transfer the money. Other than the privacy issues it entails (Preibusch et al., 2015), Paypal can suspend or reverse the transactions for any political or technical reasons. However, in Bitcoin, when the transaction is sent, no trust in a central authority or trusted party is required and the distributed consensus network will confirm the valid transaction irreversibly. This example may easily lead to the conclusion that blockchain can be considered "trust-free" by design. However, while this definition can be considered correct from a pure technical perspective—since in blockchain mathematical algorithms and cryptographic keys guarantee the integrity of the ledger rather than humans—it nevertheless overlooks the role of psycho-social factors could play in the process. Actually, as Auinger and Riedl correctly pointed out, the blockchain and its applications such as Bitcoin are not pure technical systems; rather, they are socio-technical systems (Auinger and Riedl, 2018; Castelle, 2018), that is, systems where the technological, social, and managerial components interact (Emery, 1969).

A further implication of the emergence of blockchain is that people will be increasingly required to trust non-human

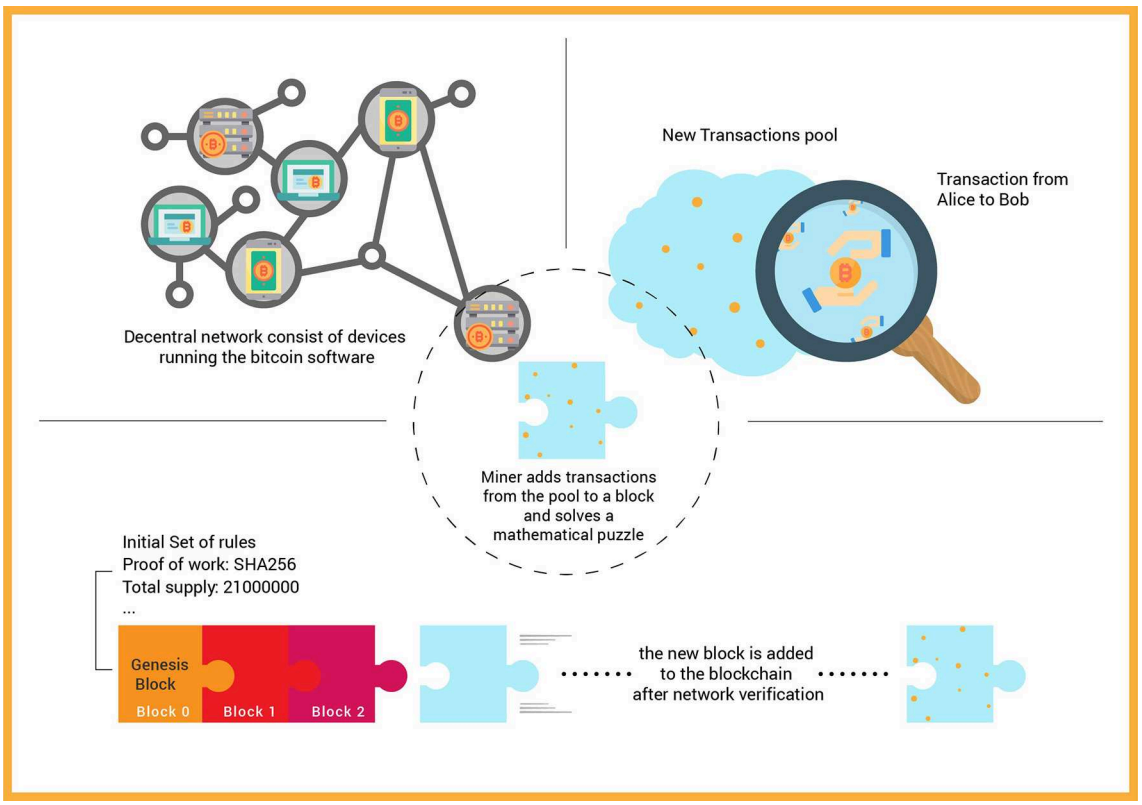

FIGURE 1 | The building blocks of blockchain technology.

entities. Actually, in a blockchain-powered world, transactions will not only happen between unfamiliar (human) parties, but also between humans and autonomous-connected devices. As an example, consider "smart contracts," a blockchain technology consisting of an algorithm and self-executing contracts with the terms of the contract between buyer and seller directly written into lines of code. Smart contracts as insurance could be used to execute/de-execute clauses that depend on a specific behavior, i.e., flight delay insurance (**Figure 2**). The contract manages the operation of an insurance-like business process. The user selects their preferred policy and pays the premium to the smart contract, when the flight lands, the smart contract gets the flight information from the airline website using Oracles (i.e., third-party agents that retrieves real-world occurrences and submit the information to a blockchain to be used by smart contracts), consequently the smart contract will calculate and transfer the payouts. In the total absence of a human-made interpretation, smart contracts require extremely accurate definitions of various circumstances and situations under which the flight schedule may occur.

Since no human intervention is involved in this process, the smart contract must guarantee to each party, e.g., that the code on which the contract is based has not been modified and is not modifiable and that the data are generated by a certified source (Eskandari et al., 2017). However, will this guarantee—enabled by blockchain—be enough for users to trust in a smart contract? One possibility is that trust in smart contracts and autonomous applications will come from the open source nature of their code, as the deployed smart contract code on a blockchain can be verified to be identical to the open source repository code. Yet trust in the open source code may still be questionable. Actually, "experts" still need to look at the code to ensure its "fairness" in that it actually does what it is supposed to do, while participants without adequate knowledge must trust in the characteristics of the open source code (Sekulla et al., 2018). This is in contrast with the legal contracts where lawyers—legal experts—verify the content beforehand or in the case of dispute, ensure a fair resolution. Another layer of trust is on the network layer in which the smart contract code is running on. Technically the trustlessness is in regard to permissionless (public) blockchains, and permissioned (private) blockchains are generally considered as trusted systems, as the entities operating the verification nodes have control over the transactions. However, if a known trusted entity, such as a bank, is running their private blockchain, does that add more trust for the users or not? This question might require further technical knowledge from the users. As depending on the implementation, the blockchain-based system can be identical to the current centralized model, or it can be toward decentralization and transparency which will add more trust for the entity in question.

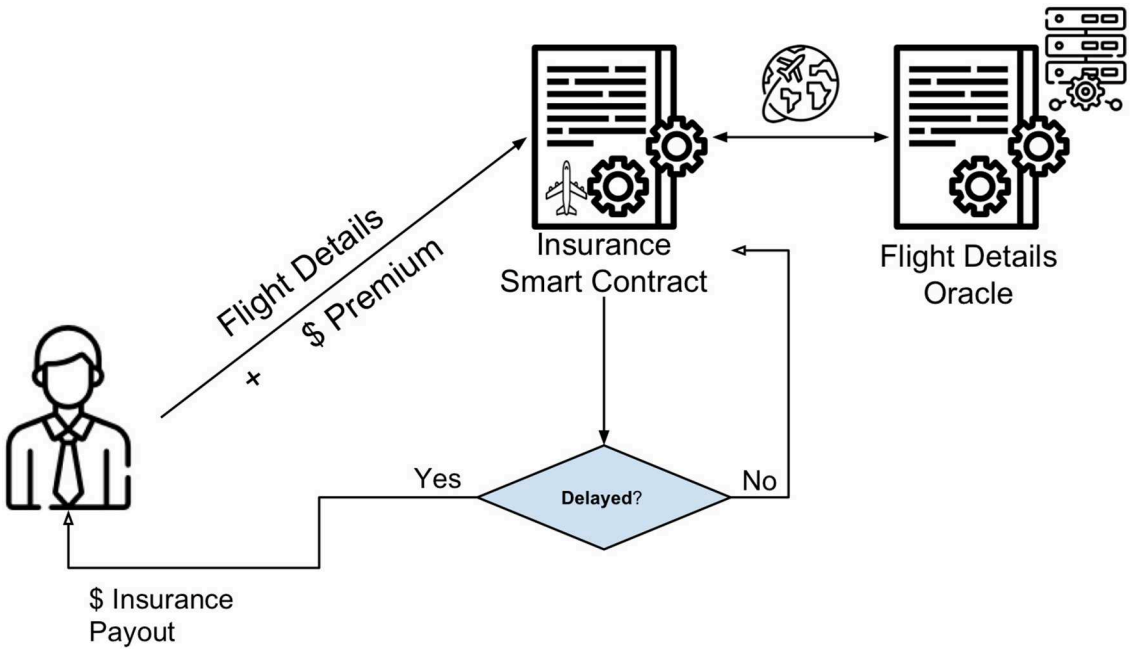

FIGURE 2 | An example of smart contract: flight delay insurance.

Blockchain-Based Systems and Trust: the Importance of the User's Perspective

The above examples stress the crucial role that user's subjective perceptions play in building trust in blockchain systems. As pointed out by Francisco and Swanson (2018), users may be reticent to use a technology if they perceive it as insecure. However, the more experience and knowledge users gain from using the technology, the more trustworthy the technology appears to them (p. 8).

Werbach (2018) proposes that rather than eliminating the need for trust, blockchain creates a new form of trust, which is added to existing "trust architectures." The first architecture is peer-to-peer trust: basically, it corresponds to the form of trust that characterizes personal relationships. The second trust architecture, which Werbach defines Leviathan trust, is the type of institutional trust that is based on the Hobbesian definition of the "social contract"—the agreement by which individuals mutually transfer their natural right. The third type, called the intermediary trust, involves a central entity that manages transactions between people (an example is the credit card system, which allows untrusting buyers and sellers to make commercial transactions). The blockchain security system, Werbach argues, enables a fourth trust architecture, in which an individual will need to trust the system as a whole, and no longer its individual components. As the author notes, on a blockchain network the three core elements that may be trusted in any transaction—the counterparty, the intermediary, and the dispute resolution mechanism—are replaced by software code, thus nothing in the system is assumed to be trustworthy, except the output of the network itself (Werbach, 2018, p. 29). However, according to Werbach, this emerging "distributed trust" architecture generates a sort of paradox: on the one hand, the blockchain relocates the agency of trust to cryptographically-secure digital ledger, thus removing the need to trust any single person or a third-party authority. On the other hand, users still *need* to trust the system for adopting it.

We hold that addressing this challenge requires a shift in focus from a purely technologically-driven view of "distributed trust," to a more user-centered perspective that stresses the importance of the users' subjective perception of risks involved in this process. Support for this claim can be found in a recent study carried out by Frey et al. (2017), in which the authors compared users' willingness to share personal data with blockchain-supported approaches to other well-established risk reduction instruments in the context of online activities. Their main hypothesis was that users would share more personal information with blockchain because the system promises to be cryptographically secure and misuse of data is practically impossible. Surprisingly, the results did not confirm this assumption, as the participants shared similar amounts of personal data regardless of whether they used blockchain-supported approaches or standard privacy policies. Furthermore, the authors found that data sharing increased for technically-affine people when they were presented with the opportunity to monetize their data. Thus, although preliminary, these findings support the notion that users' subjective perception and understanding of the blockchain security system may play a key role in determining its acceptance.

Hawlitschek et al. (2018) also recognized the importance of considering behavioral dimensions in addressing the issue

of trust in blockchain systems. They draw on and extend the blockchain engineering framework introduced by Notheisen et al. (2017) to support the analysis and design of blockchain-based platforms. The framework encompasses four layers: the *environment layer* (i.e., the social, legal and economic contexts which shape and constraints the action spaces of the other layers), the *infrastructure layer* (the technological infrastructure), the *application layer* (the set of features and rules related to a market, service or platform that affect the agent layer), and the *agent layer* (the interactions taking place between human or computer agents within the blockchain-based system). In addition to these layers, Hawlitschek et al. (2018) introduce a *behavioral layer* that is separated from the agent layer by a *trust frontier*. According to these authors, the integration of this dimension allows a behavioral perspective on the rather technical idea of "trust-free" (peer-to-peer) platforms and paves the way for a structured analysis of different targets of trust from a behavioral perspective.

A RESEARCH AGENDA FOR STUDYING THE PSYCHOSOCIAL IMPLICATIONS OF TRUST IN BLOCKCHAIN

The interest in blockchain is growing rapidly and applications of this technology are extending far beyond cryptocurrencies and monetary systems. The rapid development of this paradigm is motivated by its several advantages, which include decentralization and anonymity without the need of third-party organization in control of the infrastructure and transactions. The social, political, and economic implications of the emergence of new forms of trust enabled by blockchain could be wide-ranging: e.g., when people will start trusting in blockchain-based smart contracts, will this in turn change their trust in governments or authorities? Today citizens trust laws, police and judiciary systems not only for violent crimes but also for white-collar crimes, i.e., those violating contracts. If blockchain makes it impossible to violate a contract, why we still need to trust laws, police and justice? As a further example, consider the case of taxation (another context where trust plays an essential role, see i.e., Kirchler, 2007): if all our fiscal transactions will be traced and recorded with blockchain, are tax authorities still needed? However, as Sekulla et al. (2018) suggest, it is important to make a distinction between the early idealism and the pragmatic maturity of blockchain applications, as the real world-use of this technology requires to explore more design processes in terms of trust and develop standards for decentralized applications. While blockchain has the potential to improve the level of security of applications, building users' trust is not only a technological challenge, but also (and perhaps most importantly) a psychological one. The disintermediating nature of this technology will not downscale the importance of trust. Rather, as Sekulla et al. (2018) have pointed out, this notion will remain a central concern in the evolution of blockchain, as a key feature of the socio-technical milieu that surrounds its applications. Thus, besides technological research, psychological research is required to gain a greater understanding of people's trust in technology in the context of cryptography (Chapron, 2017). In this regard, we argue that at least three lines of research could be useful to better understand the role played by blockchain in the "trust revolution" that this technology promises:

- First, qualitative studies may explore how trust changes when it is directed toward impersonal entities, e.g., an ethnographic analysis of the meaning and values people attach to trust in different settings (e.g., traditional, interpersonal trust vs. impersonal trust in technology) might help to understand new forms of trust in non-human agents and new forms of cooperation and construction of shared meanings among the involved actors. Beside this, qualitative research can help to understand the different meanings that different populations attach to trust. As an instance, in the field of fiscal psychology, Lozza et al. (2013) found that trust in tax authorities have very different meanings for different segments of taxpayers; something similar could be explored in the field of blockchain technologies, where different segments of the population (e.g., for age, experience or expertise) could require different forms of trust and attach different meanings and values to it.
- Second, experimental studies may be carried out to examine the different levels of trust people express in interpersonal relationships vs. relationships mediated by impersonal trust in the technology. For example, in the field of behavioral economics, two typical experimental paradigms that have been used to study trust are "trust games" (Berg et al., 1995) and "public goods games." New lines of research might take advantage of these experimental paradigms to assess how trust changes when people can rely on blockchain technology. These studies could measure experimentally the level of trust in blockchain technology and the levers that can be introduced or developed in order to increase trust, as well as opportunities and constraints for trust in blockchain systems compared to traditional ones.
- Third, research is needed to inform the design of blockchain applications with design frameworks that stress the importance of human-centered values and needs. From this perspective, we argue that humanistic approaches to ICTs, such as Value Sensitive Design (Friedman, 1996; Friedman et al., 2001), Positive Technology/Computing (Gaggioli et al., 2017) and Experience-Centered Design (Hassenzahl and Tractinsky, 2006; Wright and McCarthy, 2010) may provide potentially useful frameworks to address this challenge.

These research challenges can be tackled both at individual and at organizational level. Indeed, even if private citizens will fully trust blockchain, organizational decision makers might behave in different ways: e.g., will financial organizations entrust their financial assets to a decentral network and transfer their control over to anonymous users? In conclusion, the introduction of blockchain technology has the potential to impact people' lives. While most research has focused on technological implications of this paradigm, here we argued that psycho-social aspects related to trust, identity management, acceptance, and user experience should not be overlooked. We hope that the present contribution will encourage further awareness and discussion on these issues.

AUTHOR CONTRIBUTIONS

AG and SE conceived the main idea, drafted the article, and provided final approval of the version to publish. PC and EL contributed to the writing and revision of the manuscript. All authors have made substantive contributions to the article.

FUNDING

The present work was supported by the European funded project BodyPass—API-ecosystem for cross-sectorial exchange of 3D personal data (H2020-779780).

REFERENCES

Assange, J., Appelbaum, J., Muller-Maguhn, A., and Zimmermann, J. (2016). *Cypherpunks: Freedom and the Future of the Internet*. New York, NY: OR Books.

Auinger, A., and Riedl, R. (2018). "Blockchain and trust: refuting some widely-held misconceptions," *Paper Presented at 39th International Conference on Information Systems* (San Francisco, CA), 1–9.

Beck, R., Czepluch, J., Lollike, N., and, S., Malone (2016). "Blockchain—the gateway to trust-free cryptographic transactions," in *ECIS 2016 Proceedings*. AIS Electronic Library: Association for Information Systems (AIS).

Beldad, A., De Jong, M., and Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Comp. Hum. Behav*. 26, 857–869. doi: 10.1016/j.chb.2010.03.013

Berg, J., Dickhaut, J., and McCabe, K. (1995). Trust, reciprocity, and social history. *Games Econ. Behav*. 70, 122–142. doi: 10.1006/game.1995.1027

Bowlby, J. (1969). *Attachment and Loss:* Vol. 1. *Attachment*. New York, NY: Basic Books.

Castaldo, F., Premazzi, K., and Zerbini, F. (2010). The meaning(s) of trust. a content analysis on the diverse conceptualizations of trust in scholarly research on business relationships. *J. Bus. Ethics* 96, 657–668. doi: 10.1007/s10551-010-0491-4

Castelle, M. (2018). "Relational trust, transactional assurance: socioeconomic bricolage on the blockchain," in *Proceedings of CHI 2018 Workshop "HCI for Blockchain"* (Montreal, QC).

Chapron, G. (2017). The environment needs cryptogovernance. *Nature* 545, 403–405. doi: 10.1038/545403a

Coleman, J. (1990). *Foundations of Social Theory*. Cambridge: Harvard UP.

De Filippi, P., and Loveluck, B. (2016). The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. *Internet Policy Rev.* doi: 10.14763/2016.3.427. [Epub ahead of print].

Deutsch, M. (1973). *The Resolution of Conflict*. New Haven, CT: Yale University Press.

Dunn, J. R., and Schweitzer, M. E. (2005). Feeling and believing: the influence of emotion on trust. *J. Pers. Soc. Psychol.* 88, 736–748. doi: 10.1037/0022-3514.88.5.736

Emery, F. E. (1969). *Systems Thinking*. London: Penguin.

Erikson, E. (1963). *Childhood and Society*. New York, NY: Norton.

Eskandari, S. (2015). *Real-World Deployability and Usability of Bitcoin.* Montreal, QC: Concordia University.

Eskandari, S., Clark, J., Sundaresan, V., and Adham, M. (2017). "On the feasibility of decentralized derivatives markets," in: *Financial Cryptography and Data Security. FC 2017. Lecture Notes in Computer Science*, Vol. 10323, eds M. Brenner, K. Rohloff, J. Bonneau, A. Miller, P. Y. A. Ryan, V. Teague, et al. (Cham: Springer), 11–14. .

Francisco, K., and Swanson, D. (2018). The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. *Logistics* 2:2. doi: 10.3390/logistics2010002

Frey, R. M., Bühler, P., Gerdes, A., Hardjono, T., Fuchs, K. L., and Ilic, A. (2017). "The effect of a Blockchain-supported, privacy-preserving system on disclosure of personal data," *Paper Presented at the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)* (Cambridge, MA).

Friedman, B. (1996). Value-sensitive design. *Interactions* 3, 16–23. doi: 10.1145/242485.242493

Friedman, B., Kahn, P. H., and Borning, A. (2001). *Value Sensitive Design: Theory and Methods*. UW CSE Technical Report, University of Washington.

Fukuyama, F. (1995). *Trust: The Social Virtues and the Creation of Prosperity*. New York, NY: The Free Press.

Gaggioli, A., Riva, G., Peters, D., and Calvo, R. A. (2017). "Positive technology, computing, and design: shaping a future in which technology promotes psychological well-being," in *Emotions and Affect in Human Factors and Human–Computer Interaction*, ed M. Jeon (London: Academic Press), 477–502.

Gefen, D. (2002). Reflections on the dimensions of trust and trustworthiness among online consumers. *Database Adv. Inf. Syst.* 33, 38–53. doi: 10.1145/569905.569910

Gefen, D., Karahanna, E., and Straub, D. W. (2003). Trust and TAM in online shopping an integrated model. *MIS Q.* 27, 51–90. doi: 10.2307/30036519

Gefen, D., Pavlou, P. A., and Benbasat, I. A. (2008). Research agenda for trust in online environments. *J. Manage. Inf. Syst.* 24, 275–286. doi: 10.2753/MIS0742-1222240411

Hassenzahl, M., and Tractinsky, N. (2006). Behaviour and information technology. *Behav. Inf. Technol.* 25, 91–97. doi: 10.1080/01449290500330331

Hawlitschek, F., Notheisen, B., and Teubner, T. (2018). The limits of trust-free systems: a literature review on Blockchain technology and trust in the sharing economy. *Electron. Commer. Res. Appl.* 29, 50–63. doi: 10.1016/j.elerap.2018.03.005

Hong, I. B., and Cha, H. S. (2013). The mediating role of consumer trust in an online merchant in predicting purchase intention. *Int. J. Inf. Manage*. 33, 927–939 doi: 10.1016/j.ijinfomgt.2013.08.007

Jarillo, J. C. (1988). On strategic networks. *Strateg. Manage. J.* 9, 31–41. doi: 10.1002/smj.4250090104

Kirchler, E. (2007). *The Economic Psychology of Tax Behaviour*. New York, NY: Cambridge University Press.

Lewicki, R. J., Tomlinson, E. C., and Gillespie, N. (2006). Models of interpersonal trust development: theoretical approaches, empirical evidence, and future directions. *J. Manage.* 32, 991–1022. doi: 10.1177/0149206306294405

Lozza, E., Kastlunger, B., Tagliabue, S., and Kirchler, E. (2013). The relationship between political ideology and attitudes toward tax compliance: the case of Italian taxpayers. *J. Soc. Polit. Psychol.* 1, 51–73. doi: 10.5964/jspp.v1i1.108

Mayer, R. C., Davis, J. H., and Schoorman, F. D. (1995). An integrative model of organizational trust. *Acad. Manage. Rev.* 20, 709–734. doi: 10.5465/amr.1995.9508080335

McAllister, D. J. (1995). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Acad. Manage. J.* 38, 24–59. doi: 10.5465/256727

McKnight, D. H., Kacmar, C. J., and Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: a two-stage model of initial trust in a web business. *Electron. Mark.* 14, 252–266. doi: 10.1080/10196780420002452 63

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

Newell, S., and Swan, J. (2000). Trust and inter-organizational networking. *Hum. Relat.* 53, 1287–1328. doi: 10.1177/a014106

Notheisen, B., Hawlitschek, F., and Weinhardt, C. (2017). "Breaking down the blockchain hype–towards a blockchain market engineering approach," in *25th European Conference on Information Systems (ECIS)* (Guimarães).

Preibusch, S., Peetz, T., Acar, G., and Berendt, B. (2015). "Purchase details leaked to PayPal," in *Proceedings of Financial Cryptography and Data Security 2015*, Springer Lecture Notes in Computer Science, 8975, eds R. Böhme and T. Okamoto (San Juan: Heidelberg; Springer), 217–226.

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *J. Pers.* 35, 651–665. doi: 10.1111/j.1467-6494.1967.tb01454.x

Rousseau, D. M., Sitkin, S. B., Burt, R. S., and Camerer, C. (1998). Not so different after all: a crossdiscipline view of trust. *Acad. Manage. Rev.* 23, 393–404. doi: 10.5465/amr.1998.926617

Sekulla, A., Tolmie, P., Randall, D., and Pipek, V. (2018). "Blockchain: a shift of trust," in *Proceedings of CHI 2018 Workshop "HCI for Blockchain"* (Montreal, QC).

Thielmann, I., and Hilbig, B. E. (2015). Trust: an integrative review from a person-situation perspective. *Rev. Gen. Psychol.* 19, 249–277. doi: 10.1037/gpr0000046

Thielsch, M. T., Meeßen, S. M., and Hertel, G. (2018). Trust and distrust in information systems at the workplace. *PeerJ* 6:e5483. doi: 10.7717/peerj.5483

Wang, T. D., and Emurian, H. H. (2005). An overview of online trust concepts, elements, and implications. *Comp. Hum. Behav.* 21, 105–125. doi: 10.1016/j.chb.2003.11.008

Werbach, K. (2018). *The Blockchain and the New Architecture of Trust*. Cambridge, MA: MIT Press.

Wright, P., and McCarthy, J. (2010). *Experience-Centered Design: Designers, Users, and Communities in Dialogue*. Morgan and Claypool Publishers. doi: 10.2200/S00229ED1V01Y201003HCI009

Wüst, K., and Gervais, A. (2018). "Do you need a Blockchain?," in *2018 Crypto Valley Conference on Blockchain Technology (CVCBT) (Zug)*, 45–54. doi: 10.1109/CVCBT.2018.00011

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.