Check for
updates

Understanding the creation of trust in cryptocurrencies: the case of Bitcoin

Venkata Marella[1] ⬤ · **Bikesh Upreti**[1] · **Jani Merikivi**[2] · **Virpi Kristiina Tuunainen**[1]

Abstract

Contemporary cryptocurrencies lack legal, monetary, and institutional backing that traditional financial services employ. Instead, cryptocurrencies provide trust through technology. Despite the plethora of research in both trust and cryptocurrencies, the underlying attributes of the technologies that drive trust in cryptocurrencies are not well understood. To uncover these attributes, we analyze the corpus of 1.97 million discussion posts related to Bitcoin, the oldest and most widely used cryptocurrency. Based on earlier research, we identified functionality, reliability, and helpfulness as the focal constructs with which to evaluate users' trust in technology. In our analysis, we discovered 11 different attributes related to three technology constructs that are significant in creating and maintaining users' trust in Bitcoin. The findings are discussed in detail in the article.

Keywords Cryptocurrency · Trust · Functionality · Reliability · Helpfulness · Bitcoin

Introduction

Trust is crucial to financial transactions and payments. Individuals and organizations need assurance that the transactions they make are processed and completed in a fair and safe manner, a requirement that puts financial intermediaries (e.g., commercial banks) and central banks in the business of trust (Nelms et al. 2018). These financial intermediaries guarantee the security of the customer's account and financial transactions.

✉ Venkata Marella
venkata.marella@aalto.fi

Bikesh Upreti
bikesh.upreti@aalto.fi

Jani Merikivi
jani.MERIKIVI@grenoble-em.com

Virpi Kristiina Tuunainen
virpi.tuunainen@aalto.fi

[1] Aalto University, Ekonominaukio 1, 02510 Espoo, Finland

[2] Grenoble Ecole de Management – Univ Grenoble Alpes ComUE, Grenoble, 12 rue Pierre Semard, 38000 Grenoble, France

Customers trust them and pay some amount of money as a transaction fee for their services. Unfortunately, this trust has recently been put to the test due to failures in accountability and transparency instantiated by events such as the collapse of Lehman Brothers (Montgomery 2012). Such events, which have significantly reduced people's trust in traditional financial institutions and their instruments, have led many in search of new alternatives, such as cryptocurrencies, which have gained slow but enduring popularity since the introduction of Bitcoin in 2009.

Cryptocurrencies (e.g., Bitcoin, Ethereum, and Ripple) are defined as innovative digital currencies backed by cryptography to secure and govern the transactions and supply of digital coins in circulation (Davidson and Naveed 2013). Fiat currencies, in comparison, are referred to as traditional paper-based currencies that are backed by the governments. While digital currencies are the instantiations of fiat currencies, which are used for online transactions and international transfers, there are three key characteristics that set cryptocurrencies apart from fiat currencies and their digital instantiations. First, they have no central authority, and, hence, they are claimed to be immune to government interference and manipulation. This makes them a viable alternative, especially in countries with volatile currencies and unstable economies (Scott 2016). Second, and perhaps even more importantly, cryptocurrencies draw on blockchain technology (i.e., distributed and consensus-based database with a high cryptography and transparency), which enables the use of a distributed and immutable ledger, making every transaction tamperproof – thus

eliminating the requirement of a trusted third party (Zheng et al. 2017). Third, due to their digital nature cryptocurrencies can be easily used and transferred across international borders.

Compared to traditional financial instruments, cryptocurrencies suffer from (at least) four shortcomings. First, they are not institutionally or legislatively backed; while this cuts down transaction costs, it also makes cryptocurrencies unpredictable, volatile, and risky (Brezo and Bringas 2012). Second, cryptocurrencies are typically pseudonymous, meaning that users are identified by their public key address (a 32-bit string with a combination of characters and numbers) rather than their name and social security. Consequently, this makes cryptocurrencies an easy tool for money laundering, tax evasion, and illegal trade in drugs and weapons (Brezo and Bringas 2012). Third, Bitcoin and all other cryptocurrencies are yet to obtain legal status as an investment option in many countries. Therefore, buying or selling cryptocurrencies in these countries would be extremely difficult. As such, there are several uncertainties and barriers regarding cryptocurrencies. Finally, the value of cryptocurrencies is extremely volatile for a wide variety of reasons, including cyber-attacks on cryptocurrency wallets (i.e., software that stores private and public keys needed to send and receive cryptocurrency), and exchanges (i.e., online intermediaries that help buy, sell, or exchange cryptocurrencies for other currencies).

Both digital financial services and cryptocurrencies rely on a host of underlying technologies to secure transactions, except that cryptocurrencies lack the institutional backing of a central authority. The use of cryptographic techniques increases the users' trust in cryptocurrencies, whereas traditional financial services benefit from institutional trust. In the absence of basic legal and institutional premises, cryptocurrencies demand trust, not in people but in technology (Jarvenpaa and Teigland 2017; Ostern 2018) as the security of financial transaction depends upon the underlying technology. The increasing popularity of cryptocurrencies implies that there are still millions of enthusiasts who are willing to trust in the underlying technology and go on to use or at least experiment with cryptocurrencies.

Despite the wealth and diversity of research on cryptocurrencies and trust in technology (Lankton et al. 2014), only a few studies have hitherto examined trust and technologies within the cryptocurrency domain, which is devoid of any institutional backing and human intervention (Walton and Dhillon 2017). What is still not fully understood is what attributes lead to individuals' trust in different technologies related to cryptocurrencies, including blockchain, cryptocurrency wallets, and exchanges, when applied to a particular purpose. In other words, what are the attributes that facilitate creation of trust in cryptocurrencies and related technologies? Bridging this gap is of crucial importance since the locus of trust is shifting from people to technology, we need to understand the attributes of the technology that can replace the human component of trust (Jarvenpaa et al. 2019; Lindman et al. 2017). Moreover, the use

of technologies creating the cryptocurrency transactions must come with low risk and uncertainty, just like any other financial transactions (Li et al. 2008). Yet, understanding what specific attributes of technology increase trust comes thus with a managerial implication: technology designers and business professionals need to be aware of which technology attributes are perceived as most relevant by both existing and potential users. This kind of understanding can also be of interest in other domains, such as governance (e.g., voting and taxing) and healthcare (e.g., incorruptible medical data), where reliable technology is of utmost importance (Beck et al. 2017).

This paper is organized as follows. First, we offer a brief introduction to cryptocurrencies and the underlying technology. We then adopt a theoretical framework, which links trust in technology to three constructs: functionality, helpfulness, and reliability (Lankton et al. 2014). We use these constructs to better understand what generates trust around cryptocurrencies. In terms of empirical evidence, we focus on Bitcoin, as it is the most popular and most widely used cryptocurrency (Lindman et al. 2017). To understand how trust links to technology, we analyze a corpus of 1.97 million posts extracted from a popular cryptocurrency forum (Bitcointalk.org). Our analysis of the Bitcoin-related posts builds on the text content model, which employs doc2vec, a neural-learning model for text data developed by Le and Mikolov (2014). The results report on technological attributes semantically closest to the trust construct, which helps us to understand the attributes of the technology that create trust in cryptocurrencies among the users. We will conclude our paper by discussing the main findings and their implications for research and practice. We also identify potential limitations and future research opportunities.

Background

Underlying technology

Cryptocurrencies rely on three technological elements: blockchain, cryptocurrency wallets, and exchange platforms. Of these, blockchain technology forms the backbone of cryptocurrencies. It can be defined as a decentralized and distributed database that is shared across a network of computers called nodes (Narayanan et al. 2016). Each node in the network has access to the data on the blockchain. Each block contains a unique identifier termed a hash, which is determined by the content of a block and is inputted to the next new block. A new block, which is created every ten minutes, contains the hash value of the previous block and transactions of the current block. Backdating, revising, tampering, or deleting any of the blocks will also change the hash value, which then creates a mismatch between the blocks in the blockchain. This property of the blockchain makes it a trusted network, since changing block data would require changing the hash

value of every subsequent block and this must be computed faster than other nodes in the network before they can add new blocks to the chain. The following simplified diagram represents the data structure of the blockchain technology (Fig. 1).

A cryptocurrency wallet is a software program that stores the public and private keys of an account and can interact with blockchain to enable the management of the account. Cryptocurrency wallets can be either stored on a hardware device, or a wallet software that can be saved either on the computer or an exchange. These wallets facilitate the transfer of cryptocurrencies from account to another account easily (Bierer 2016). A cryptocurrency exchange is a web-service that provides its customers with services for the exchange of cryptocurrencies into various assets such as fiat or other digital currencies (DeVries 2016). Exchanges buy the cryptocurrencies from sellers and then sell them to buyers. Examples of reputed exchanges include Coinbase, Kraken, and Bitstamp, to name a few Fig. 2.

Trust in technology

Trust refers to the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform an action important to the trustor, irrespective of the ability to monitor or control that other party (Mayer et al. 1995). Trust is a dynamic concept that develops over time (Luna-Reyes et al. 2004). It is an individual's reliance on another person under conditions of dependence and risk (Kramer and Tyler 1996). Reliance allows another person to take control of one's assets. A trustor is someone who holds certain expectations about the other party, while the trustee is a person or an entity that is assessed by the trustor (Becerra and Gupta 2003).

While trust has been studied extensively and from varying perspectives (McAllister 2018; de Ruyter et al. 2001), also in IS research (Jarvenpaa and Todd 1996; Pavlou and Gefen 2004), research on trust in technology is still in its infancy, despite being very much in demand. McKnight et al. (2011), for example, note that besides building trust in other actors

(e.g., sellers and buyers) and agents (e.g., operators and intermediaries), users tend to also trust (or not to trust) technology. While trust in technology excludes moral volition, as technology has typically left moral conduct and decision-making to its users, this seems to hold especially true when technologies, such as blockchain or other automated technologies like autonomous vehicles, eliminate the necessity of having a human intervention in the process. With these technologies, users are left vulnerable to the capacity of technology to help achieve their goals (e.g., A smartphone user trusts that the smartphone connects well to the internet). Therefore, the question of what makes individuals regard technologies as trustworthy remains poignant.

Mcknight et al. (2011) divide the trust in technology construct into three concepts: a) propensity to trust general technology, b) institution-based trust in technology, c) trust in a specific technology. Propensity to trust general technology refers to individual's willingness to depend on different technologies in different situations (Mayer et al. 1995). Individual's propensity to trust general technologies depends on his/her faith in general technologies and trusting stance. Faith in general technologies refers to individuals' beliefs about technological attributes while trusting stance is about the belief that relying on the usage of a particular technology would result in positive outcomes (Mcknight et al. 1998).

Institution-based trust in technology refers to the belief that the supportive situations and structures tied to a specific class of technologies within a specific context would make the technology successful. Institution-based trust in technology consists of situational normality and structural assurance. Situational normality-technology refers to the belief that using a specific class of technologies in a new way is normal while structural assurance refers to the belief that adequate support is provided for the successful use of technology in terms legal, contractual, or physical support (Mcknight et al. 1998).

Trust beliefs in technology refer to the beliefs about the favorable attributes of a specific technology (Mcknight et al. 2011). According to Friedman, Khan, and Howe (2000, 36),
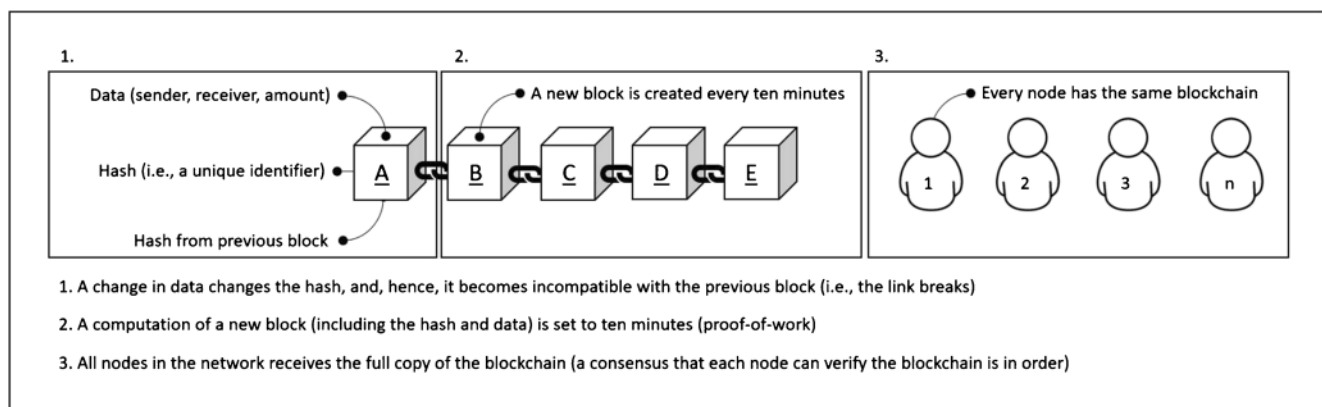

Fig. 1 A simplified representation of a blockchain data structure (Narayanan et al. 2016)
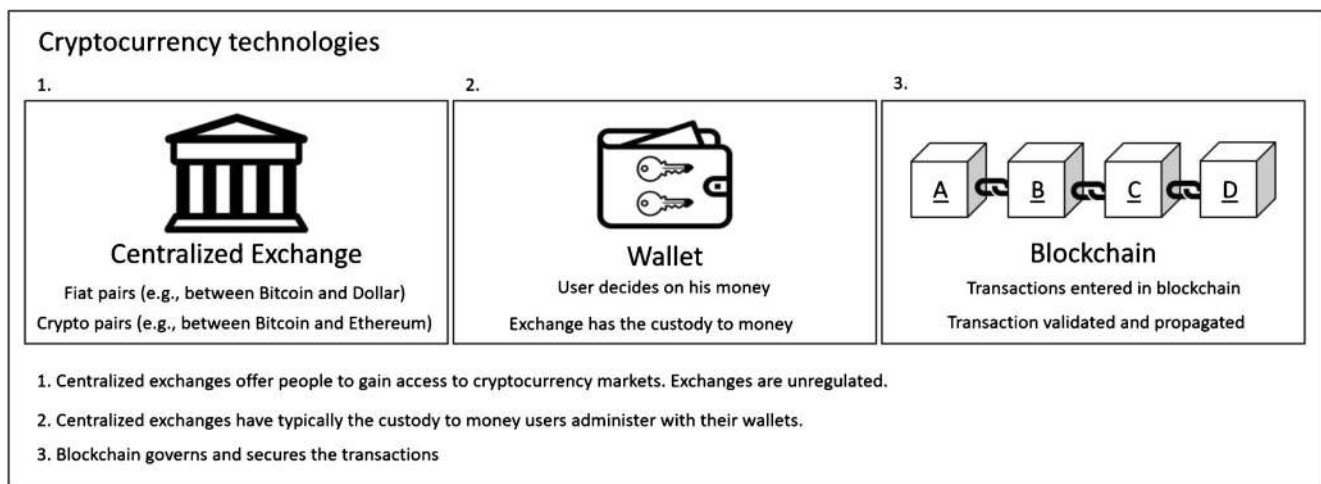
Fig. 2 Cryptocurrency Technologies (Narayanan et al. 2016)

"people trust people, not technology". However, if technology resembles the qualities of humans, then people trust technology. The current literature on trust beliefs in technology employs two different sets of trust constructs. The first set consists of human-like trust constructs, such as benevolence, integrity, and ability. The second set of constructs are system-like constructs, such as helpfulness, reliability, and functionality (Lankton et al. 2014). While benevolence, integrity, and ability are the trust constructs related to humans, these characters would translate into helpfulness, reliability, and functionality when it comes to trusting the attributes of the technology. The underlying idea behind associating these trust constructs to technology is that they reveal which attributes of technology add value (Mcknight et al. 2011). Thus, if a user believes that blockchain better survives malicious attacks because of its decentralized nature, then it is likely that the user perceives this attribute to add to blockchain's trustworthiness, and, consequently, its value (Thatcher et al. 2011).

Concerning the three trust constructs - functionality, helpfulness, and reliability - proposed by McKnight et al. (2011) and empirically validated by Lankton et al. (2014), competence/ability refers to the belief that the trustee has skills that help the trustor achieve the desired function (e.g., a translator with an ability to translate texts from one language to another language). In the case of technology, functionality is conceptually very similar to ability or competence. Functionality refers to the belief that a specific technology has the capability, functions, and features, to do the required task (e.g., software that translates texts from one language to another). Integrity is the belief that a trustee associates with a set of principles that are acceptable to the trustor (e.g., a translator who translates texts from one language to another during office hours). On the other hand, we have reliability that represents the integrity aspect of trust in technology. Reliability can be defined as the property that enables technology to operate consistently over a period of time (e.g., software that

translates texts from one language to another at all times). Benevolence is the belief that trustee is motivated to do something good for the trustor, besides being profitable (e.g., a translator who besides translating texts from one language to another during office hours, offers advice about where to take the texts that need be translated outside office hours). Helpfulness is like benevolence and is described as the belief that technology provides adequate and responsive assistance to users via their help attributes (e.g., software that, besides translating texts from one language to another at all times, provides guidance on how to enable the speech recognition attribute). Table 1 presents the three constructs.

In this study, we adopt the above three constructs and utilize them in identifying the underlying attributes of the cryptocurrency technologies (i.e., the blockchain, cryptocurrency wallet, and exchanges) described earlier in this section. We acknowledge that individuals intending to use, and those already using, cryptocurrencies may have different expectations about these technologies than those using them for other purposes (i.e., attributes that cryptocurrency users trust in these technologies may not be the same attributes that actors in the music industry, who care about intellectual property rights, trust in them). Thus, the attributes linked to these trust constructs are context-dependent, which is because the uncertainty that technology creates for users depends on these user's goals. To tap into this contextualization, we seek to identify the key trusted attributes of technologies with user-generated data over the years, which would help us uncover trust characterized as persistent.

Method

In this section, we will describe our data collection process from the popular online Bitcoin forum. Thereafter, we elaborate on our methodological approach and techniques.

Table 1 Constructs of Trust in Technology (Lankton et al. 2015)

Constructs	Human-like comparison	Description	Operations
Functionality	Ability	Functions needed to accomplish the expected tasks	Performs a function for the user, provides system features the user needs to do a task, provides the user with the appropriate functionality
Reliability	Integrity	Continually operating properly or in a flawless manner	Performs functions reliably, does what the function says it will do, gives accurate and unbiased facts and information, calculates correctly, does not crash
Helpfulness	Benevolence	Providing adequate and responsive aid	Provides help, understands and caters to needs, does not cause harm, is responsive to user needs and requests

Data collection

Our objective is to understand how Bitcoin has generated trust among its users despite being anonymous and devoid of any legal and institutional backing. In this context, discussion forums have played a crucial role in the growth of Bitcoin, as users engage in the discussion and interaction to share knowledge and information. Among various online discussion forums, "Bitcointalk.org" is one of the oldest and most popular online forums, and it has a large user base. This online forum was started by Satoshi Nakamoto for the purpose of communicating with other developers (Nakamoto 2009a, b). As of September 2019, Bitcoin Forum has over 2.6 million members posting 52 million posts on 1.21 million topics ("Bitcoin Forum - Statistics Center" 2019; Table 2).

In addition to BitcoinTalk forum, there are also several other similar online forums (e.g., Cryptocurrency Talk, Bitcoin Garden, and Bitcoin Stack Exchange), which are considered useful forums focused on cryptocurrencies (Crytalker 2019). However, BitcoinTalk forum outperforms the other online forums in terms of number of users, posts, and topics ("Bitcoin Garden Forum-Statistics Center" 2019; "Cryptocurrency Talk" 2019; "Bitcoin Stack Exchange" 2019).

We base our analysis on the Bitcoin-related discussion posts collected from BitcoinTalk forum for two important

Table 2 Descriptive Statistics of BitcoinTalk Forum ("Bitcoin Forum - Statistics Center" 2019)

General statistics of Bitcointalk forum	
Total Members	2663701
Total Posts	52398770
Total Topics	1216200
Total page views	4795109378
Average registrations per day	398.21
Average posts per day:	7310.46
Average topics per day	294.41
Average online per day	168.12
Male to Female Ratio of members	4.7:1
Average page views per day	1336429.59

reasons. First, compared to other data sources mentioned in Table 3, online discussion platforms serve as a good alternative to source data, as discussions, interactions, opinions, and the flow of information can be accessed on an unprecedented scale. Second, discussion data do not condition the study or experiment that is being conducted; rather, they are naturally generated by the users. This allows us to infer the technological attributes related to trust in Bitcoin from the users' own words and statements, which were used to address their concerns or share information within the Bitcoin community.

To collect data from the discussion forum, we wrote a web scraping script using Python package *beautifulsoup*.[1] As our objective is confined to Bitcoin, we limit our analysis to general discussions on Bitcoin covering four subtopics of legal, press release, meetups, and important announcements. We downloaded close to 1.97 million discussion posts written between March 1, 2012, and September 21, 2018. Our data included original posts and replies to them, dates of each post and reply, and the metadata about the users who posted.[2]

Text modelling

Our aim was to identify the technological attributes that have contributed to the creation of trust among Bitcoin users. The first step in this direction required us to identify the relevant posts. A naïve approach would have been to use a simple keyword search to retrieve trust related posts. However, such an approach entails two fundamental issues. First, discussion posts are user-generated data, where users are not obliged to adhere to the grammatical form and correctness. Further, users can use a combination of words to mean trust. Second, in the context of large data, a keyword-based search, for example, trust related search, can easily return tens of thousands of posts. Even with this large number of search results, the search would fail to include the posts with words such as faith, belief, and reliability, which are concepts similar to trust. Further, identifying relevant posts would require manually reading all posts, which would have been impractical with the volume of

---

[1] https://pypi.org/project/beautifulsoup4/
[2] We are willing to share our data for academic research purposes.

Table 3   Comparison of various Online Forums

Measure	BitcoinTalk Forum	Cryptocurrency Talk	Bitcoin Garden Forum	Bitcoin Stack Exchange Forum
Total Number of Members	2,663,701	90,098	26,033	67,212
Total Number of Posts	52,398,770	456,113	429,913	NA
Total Number of Topics	1,216,200	111,779	55,147	22,922

data we had. Moreover, any kind of ordering of the posts would be a difficult task, considering it requires the development of a consistent and reliable scoring method to measure the trust related content in the post. Any use of such method would require overcoming the variance among the persons scoring the posts.

To circumvent these issues, we relied on the vector representation of words and documents generated through paragraph vector, also known as *doc2vec*, proposed by Le and Mikolov (2014). After the vector representation, we computed the semantic similarity to identify the closeness of the posts and words to trust. Semantic similarity is a metric defined over the corpus, where the similarity is based on the likeness of their semantic meaning instead of the syntactical representation. In terms of learning semantic similarities, doc2vec methods have demonstrated superior performance to competing methods, such as bag of words (Dai et al. 2015; Le and Mikolov 2014). The root of the paragraph vector method lies in the usage of a neural network in predicting the word near the word. In this neural network-based method, a vector of weights is trained to maximize the prediction of the nearest word for a word in a given context. Like a classification problem, the model learns the network weight in order to maximize the prediction of the nearest word. However, unlike the classification problem, these networks output the learned weight as a vector and semantic representation of the text rather than the final prediction from the model. These vectors - word embeddings - are considered a good representation of the text as they capture semantic similarities by contributing to the nearest word prediction task. Mikolov et al. (2013) reported state-of-the-art performance in learning semantic similarities and relationships. For instance, the word vector method could produce a relationship such as "King – Man + Woman = Queen" (Mikolov et al. 2006). The semantic meaning of the word "king" refers to leadership and also refers to the gender as male. If you remove the semantic meaning of "Man" (which is Male) in the word and add the semantic meaning of the word "Woman" (which is female), then you are semantically left with the concept of leadership and female. This combination of female and leadership is represented in word form as "Queen". Later, this idea was extended by Le and Mikolov (2014) as a paragraph vector, also known as doc2vec, which could learn the semantic representation for both the words and documents in the same vector space. Their approach involved important improvements, including

the ability to retain word order, and also allowed the text of variable length.

To train doc2vec model, we relied on the implementation provided by Python package *Gensim* (Rehurek and Sojka 2010). Among available models, we trained three different variants of the doc2vec model: paragraph vector with a distributed bag of words (PV-DBOW) with doc vectors only, PV-DBOW in a skip-gram mode with word vectors trained with document vectors, and PV- with distributed memory (PV-DM) using the sum. Due to the huge resource requirements involved in estimation PV-DM with concatenation, we omitted it from our potential model alternatives. In training all three doc2vec models, we set the same model parameters: vector size to 300 dimensions; context window size of 10; minimum word frequency to 5; and epochs to 50. Here, vector size refers to the dimension of vector outputs for both word and document vectors. Similarly, context window size refers to the length (number of words) that is considered as a context. Here, while learning the semantic relationship, our model considered 10 words at a time in a sliding fashion for each document. Given that the post could be of varying length, we considered the context window size of 10 to be a reasonable choice. Similarly, an epoch refers to the number of training iterations. We trained our models with 50 iterations, well above the practice of 10 iterations. After training models, we manually evaluated the word and document similarity in randomly selected 20 words. The results showed that paragraph vector with a distributed bag of words with documents and words trained together performed better in comparison to other models, making it our preferred choice.

Figure 3 summarizes the methodological approach used in the analysis of the discussion posts collected from Bitcointalk. org. Our methodology included cleaning and pre-processing the text, followed by training the doc2vec model. Once the model was trained and the preferred model selected, we analyzed the data, building on two sets of output from doc2vec model: 1) word vectors: semantic representation of words in the collection of posts; and, 2) document vectors: semantic representation of the actual posts. To analyze the data, we first extracted fifty posts closest to the keywords related to the constructs - reliability, functionality, and helpfulness. Given a word as input, the doc2vec model can return similar document - words with a similarity score using cosine similarity. Cosine similarity is computed over the vector representation of the given words, and the closest word or document vectors
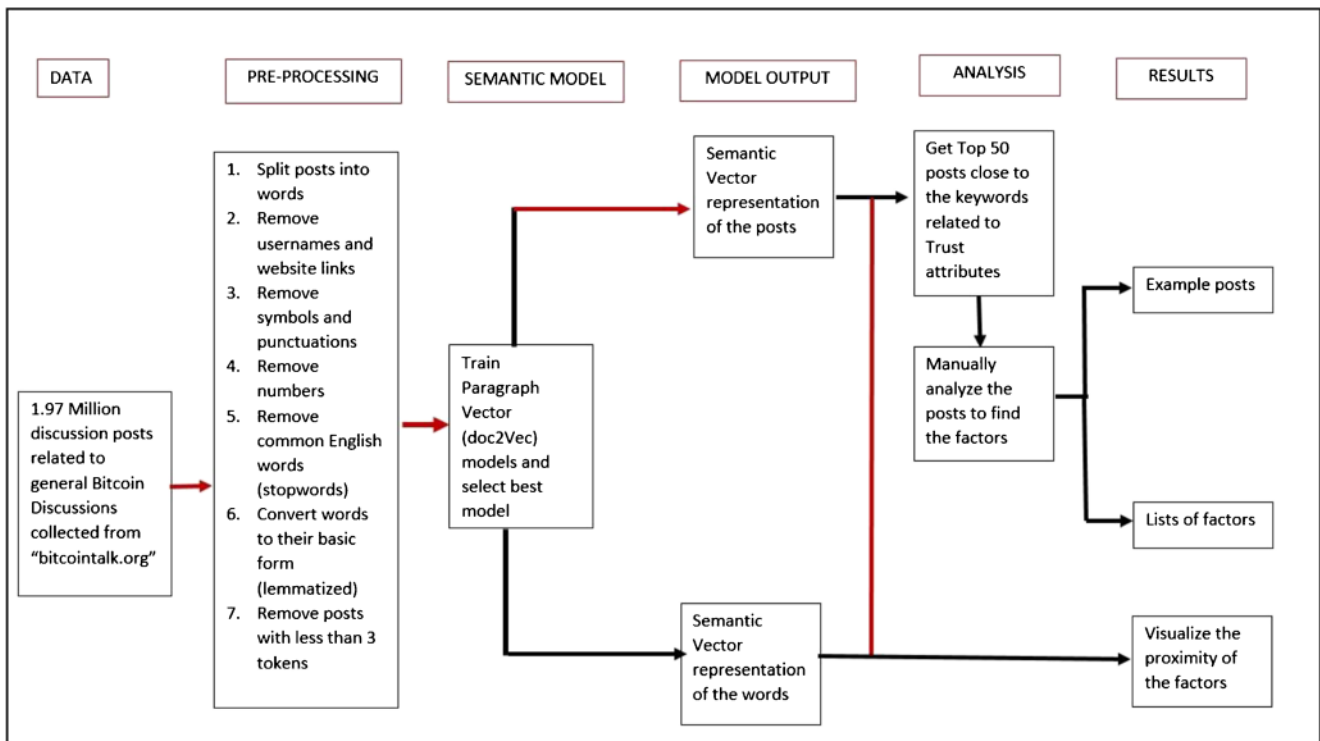
Fig. 3 The Methodological approach used in the analysis of data

with the highest cosine similarity score is returned. Since these vectors are learned from data exclusive to Bitcoin discussions using several context windows with the given words, we deemed it as a suitable method to extract relevant posts.

Once the posts were collected, we read through them to identify the technological attributes. Moreover, to understand the semantic proximities between the words, we first computed the pairwise similarity and then visualized it as a network of words. The pairwise similarity matrix gives a similarity score between the pair of words, whereas visualizing it as a network allows us to see the relative positions between the attributes when all the pairwise similarity are considered. These relative positions of the words, as the node in the network, allows us to see the semantic proximities between the word vectors. We will present our results using descriptions of the identified attributes with example posts in the following section.

Results

Our analysis builds on the output from doc2vec model of discussion posts. To identify the attributes of Bitcoin related to trust, we first extracted fifty most similar posts to the keywords related to the trust-related constructs - functionality, reliability, and helpfulness. To search for the constructs, we listed the keywords representing functionality, reliability, and helpfulness in the context of blockchain technology and cryptocurrencies, from the literature. For instance, to represent

functionality, we searched for keywords such as transfers, decentralization, immutability, and openness. Similarly, to identify *reliability*-related posts, we searched for posts closest to the keywords stability, regulation, knowledge, and security. Finally, we used keywords, such as investments, profits, and alternative currency as words associated with the *helpfulness* construct. We derived these keywords from the literature, as elaborated on in Table 5 in the Appendix section. Apart from these keywords, we used some synonyms of functionality, reliability, and helpfulness in the context of cryptocurrencies. The most similar posts were based on the similarity score between the word vector of the constructs and the posts. Using these keywords with the doc2vec model, we extracted the top fifty posts for each keyword. We read through and analyzed these 850 posts and found eleven attributes relating to the three constructs functionality, reliability, and helpfulness. Table 4 lists the attributes with descriptions and similarity scores. The table also links the attributes to trust constructs related to functionality and reliability to the technology or technologies that are exclusive to Bitcoins and cryptocurrencies. The table links the three technologies of focal interest - blockchain technology, cryptocurrency wallet, and cryptocurrency exchange - to the trust-related attributes. Finally, we note the similarity with the given keywords and the content of the post with a similarity value mentioned next to the post. A similarity value of one means that the post is exactly like the keywords, while a similarity value zero denotes that post is not like the given keywords at all.

Table 4 Constructs of Trust in Technology * Similarity value expresses how semantically similar the attributes (keywords) are to the words the given post contains

Constructs	Example post [similarity value]*	B**	W**	E**
Functionality				
Transfer (ease and affordability of transactions)	*"Bitcoin is better than cash because it can be transferred easily." [0.64]*		X	
Decentralization (shared ledger)	*"I believe, bitcoin is more valuable. Because it is trusted, decentralized, our interest and our investment in bitcoin which makes it valuable." [0.65]*	X		
Immutability (tamperproof ledger)	*"Bitcoin will never end or will never be destroyed. The system is secure and the blockchain is immutable and more and more people are joining the network to make it better." [0.54]*	X		
Openness (Public Ledger)	*"The openness is striking. This is the kind of thing we need in this economy. Security and transparency. Thanks for sharing this." [0.54]*	X		
Reliability				
Stability (high volatility)	*"The main factor that scares people from investing in it is the risk factor. People find it risky because Bitcoin's price is not steady...."[0.63]*		X	X
Regulation (regulations helps cryptocurrencies promotes trust and reliability)	*"Bitcoin can never die regulation can only make it to be strong and trusted by many people." [0.63]*	X		
Security (hacking, stealing, and fraudulence)	*"[...] My BTC address from Zebpay account having almost 0.01550 BTC has been hacked and the amount has been stolen just few days ago....." [0.61]*		X	X
Knowledge (simplicity/complexity of cryptocurrencies)	*"Knowledge and understanding will keep people in getting into cryptocurrency because definitely he can understand analyse....." [0.61]*	X	X	X
Helpfulness				
Investment (value expectations)	*"I mainly use bitcoin as investment for future and sometimes I purchase goods with bitcoins." [0.66]*			
Profits (Earn profits in a short period)	*"The main advantage for me-with the help of investments in bitcoin, you can earn quite a large amount of money."[0.59]*			
Alternative Currency (to fiat currency)	*"This is the great news for iran and uzbekistan. as they are consider as third world country. They are mainly suffering from currency .." [0.58]*			

The closer the value is to one (1), the higher the similarity; ** B = blockchain, W = wallet, and E = exchange

Our findings suggest that coin transfers, immutability, openness, and decentralization are the functional attributes of Bitcoin, responsible for creating trust among the users. Many users felt that transferring Bitcoins is much easier and quicker than transferring fiat money. Immutability in Bitcoin means the transaction histories recorded on Bitcoin blockchain cannot be manipulated, deleted, or revised (Low and Teo 2017). Similarly, openness refers to the property that the information on the blockchain is available to the public. The attribute of having a robust publicly available distributed blockchain creates trust among Bitcoin users (Berke 2017). The decentralized structure, openness, and immutability are the unique attributes of the blockchain technology and are major attributes contributing to trust creation among Bitcoin users.

In terms of reliability, we found that attributes such as stability, regulation, security, and knowledge of Bitcoin would make it a reliable technology. Bitcoin is often criticized for its volatility (Bouoiyour and Selmi 2006), with users expressing concerns about volatility in its value. They believed that the stability in the value of Bitcoin would make it more reliable. Second, contrary to a certain segment of the user beliefs, many users believed that regulations would make Bitcoin more reliable and, thus, would convince many others to use it. According to the legal experts (Kaplanov 2012), Bitcoin would flourish under legal regulation. Third, users were also worried about the security of the wallets and cryptocurrency exchanges due to the cyber-attacks on various wallets and exchanges. During the first half of 2018, cryptocurrencies worth 1.1 billion dollars were lost in cyber-attacks (Rooney 2018). Improved security measures by exchanges and individual wallet holders will make Bitcoin more reliable. Finally, users with a better understanding of the technology behind Bitcoin felt more secure about it. They understood the situation better and were able to make a better investment decision to gain bigger profits.

With regard to attributes related to the helpfulness of Bitcoin many users agreed that it was a great investment tool to earn profits in the short term. The acceptance of Bitcoin as a payment system is yet to evolve completely (Pollock 2018). Most users considered it helpful as an investment option rather than a payment tool. Finally, Bitcoin turned out to be an alternative currency for people living in countries with volatile fiat currency. Though Bitcoin is highly volatile, the technology makes it possible to buy them easily. Hence, it serves as an alternative currency in those countries.

Once the trust-related technological attributes were identified from the posts, we explored their semantic closeness to trust. We, therefore, plotted the word vectors of these attributes with the word vector of trust. As the vector representation from the model

allows mathematical operations, we can use these vectors to compute semantic similarities. To analyze semantic proximities between attributes, we first computed pairwise cosine similarities between the eleven attributes and trust. Cosine similarity is a metric that measures a cosine angle between the vectors and assigns the similarity score based on the direction of vectors. For instance, vectors that point to the same direction are deemed similar whereas vectors that are orthogonal (angle of 90 degrees) are dissimilar. The similarity score ranges from one, for similar vectors, to zero for the dissimilar ones. Next, to explore the semantic proximity we represent the pairwise similarity matrix as a network graph. A pairwise similarity matrix (see Table 6 in the appendix) lists out the similarity score between the pairs. However, in the actual post, most of these attributes are likely to be discussed in relation to each other and thus, are related to each other in more than one way. For instance, in the pairwise similarity matrix, attributes like immutability and openness have a low similarity score. But, these attributes are closer to decentralization which in turn is close to "Alternative currency", which is closer to the trust vector. In the context where these attributes are related to each other in multiple ways, a pairwise similarity matrix alone cannot fully capture semantical proximity between attributes. Thus, we analyze semantic proximities between the attributes with the use of semantic proximity network where the pairwise similarity between the attributes is presented as a network graph. Figure 4 depicts the semantic proximity network where the positions of attributes are determined after considering the relative positions of all the attributes. The figure shows that the use of word "Trust", in the context of Bitcoin discussion, is semantically closer to attributes like transfer, immutable, and openness. Additionally, the network graph also shows some

interesting grouping of attributes like technical aspects of the blockchain (openness, immutability, and security), financial (alternative currency, profitability, investment, transfer, and regulation), and information systems and other important requisite (knowledge, regulation, decentralization).

Discussion and conclusion

Cryptocurrencies are a relatively new phenomenon that can potentially bring radical changes to digital markets on a global scale. Many banks and other traditional financial institutions initially wary of cryptocurrencies and their underlying logic, are now planning to introduce their own cryptocurrencies (Woodford 2019). We see that cryptocurrencies are starting to put pressure on digital currencies. This said, our study provides valuable insights for scholars and business practitioners alike to understand what creates trust in cryptocurrencies.

Our aim in this study was to examine and identify technological attributes that contribute to creating trust among the users' in the cryptocurrency domain. To do this, we employed the technology trust model proposed by Lankton et al. (2014) and focused on three distinct trust constructs: functionality, reliability, and helpfulness. We used these constructs to identify the specific attributes that contribute to trust in the technologies underlying cryptocurrencies (i.e., the blockchain, cryptocurrency wallet, and exchanges). As for the empirical analysis, we decided to focus on Bitcoin, because it is the oldest and the most widely used cryptocurrency in the market. To collect data, we extracted 1.97 million posts from a popular cryptocurrency forum Bitcointalk.org. The analysis drew on a

Fig. 4 Semantic Proximity Network representation of Trust and the associated attributes
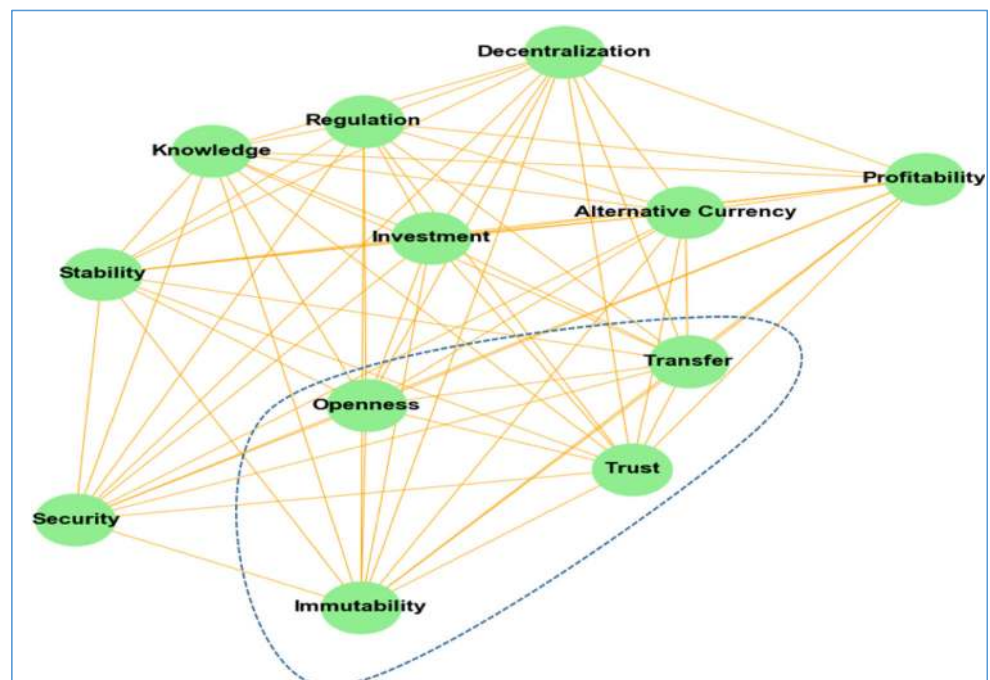
paragraph vector model termed doc2vec (Le and Mikolov 2014), which produces a semantic representation of words and posts. This allowed us to map the semantically most relevant attributes with the three trust constructs.

We identified 11 attributes that impact the trust in cryptocurrencies. Among these 11 attributes, trust is semantically close to transfers, immutability, and openness, of which immutability and openness are the unique attributes of the cryptocurrencies using blockchain technology. Cryptocurrencies, such as Bitcoin, could make international transfers much easier, with lower transaction fees than those charged by traditional commercial banks (Bamert et al. 2013). Since cryptocurrencies could become an alternative method for international money transfers, many commercial banks are looking into launching their own cryptocurrencies. The other attributes that are semantically close to trust are ledger immutability and openness - the former securing safe and fair transactions and the latter making the transaction information accessible to the public. Immutability means that the transaction history provided on Bitcoin ledger cannot be manipulated, revised, or deleted by anyone. Openness refers to the availability of the data on the Bitcoin blockchain to everyone, rendering the system completely transparent. Openness creates transparency, while immutability creates accountability. Transparency is considered as the key element in trust creation (Grimmelikhuijsen et al. 2012). These two functionalities are the unique attributes of cryptocurrencies using Blockchain technology. The degree of transparency and accountability offered by Bitcoin or other cryptocurrencies is unparalleled to that of any traditional financial institution. When technology provides high enough level of transparency and accountability, it eliminates the necessity of a trusted central authority to govern the system. In other words, it is essentially the core properties of blockchain technology that facilitate the creation of trust in cryptocurrencies.

Our research makes four important contributions to the literature related to trust in cryptocurrencies. First, we identified the trust-creating attributes of cryptocurrencies that utilize blockchain technology. Second, we identified the technological attributes that can replace the human component of trust in business transactions. These are attributes afforded by technologies, such as blockchain that can create trust among the participants of business transactions by offering high degree of transparecy and accountability through an open and immutable ledger. Third, we demonstrated the usefulness and functionality of large-scale data from the Bitcoin community combined with state-of-the-art textual analysis as a research methodology in studying the attributes that generate trust in technology. Finally, we believe that our results can be generalized beyond cryptocurrencies to other blockchain-based applications. As many blockchain-based applications are still in their early stages of development, it is crucial for the business owners to understand the attributes that create trust among the users, and our findings can help in that.

Like all research, our study has certain limitations. We acknowledge that the membership of the forum includes both the actual Bitcoin users as well as non-users. Hence, the trust attributes of technology that we identified from the textual analysis were not exclusively based on the opinions of actual users with real experience with Bitcoin. Secondly, we do not have information on the forum members' technical skills or understanding about the blockchain technology. Accordingly, our findings reflect the views and opinions of people with different levels of interest and experiences with cryptocurrencies in general and Bitcoin in specific; and with different levels of technical skills and knowledge. In the future, we hope that researchers in this area will analyze the relationships between the identified trust attributes and the level of their technical skills. This will provide a deeper understanding of trust-related technological attributes that encourage or hinder the use of blockchain and its applications, such as Bitcoins.

Appendix

Table 5 Keywords for the constructs from the literature

Construct/ Keywords	Description	Reference
Functionality Payments	"Bitcoin is increasingly used in a number of 'fast payment' scenarios, where the exchange time between the currency and goods is short" Page - 907	Karame, G. O., & Androulaki, E. (2015). Double Spending Fast Payments in Bitcoin Categories and Subject Descriptors. ACM Transactions on Management Information Systems, 18(1), 906–917
Electronic Transfer	"Bitcoin success is mostly due to the innovative use of a peer-peer network to implement all aspects of a currencies lifestyle, from creation to its transfer among the users." Page - 978	Decker, C., Decker, C. and Wattenhofer, R. (2016) 'Information propagation in the Bitcoin network Information Propagation in the Bitcoin Network', 13-th IEEE International Conference on Peer-to-Peer Computing, (August), pp. 1–10. doi: https://doi.org/10.1109/P2P.2013.6688704

Table 5 (continued)

Construct/ Keywords	Description	Reference
Immutability	"Bitcoin's distributed, verifiable, and immutable public transaction ledger, known as the blockchain, holds out the promise of fast, cheap, peer-to-peer financial transactions." Page - 220	Folkinshteyn, D. and Lennon, M. (2016) 'Braving Bitcoin: A technology acceptance model (TAM) analysis', Journal of Information Technology Case and Application Research. Routledge, 18(4), pp. 220–249. doi: https://doi.org/10.1080/15228053.2016.1275242
Decentralization	Bitcoin is a completely decentralized system with no server or central authority as everything is validated by cryptography.	Maurer, B., Nelms, T. C. and Swartz, L. (2013) '"When perhaps the real problem is money itself!": The practical materiality of Bitcoin', Social Semiotics, 23(2), pp. 261–277. doi: https://doi.org/10.1080/10350330.2013.777594
Openness	Bitcoin is a new class of the accountable system, which allows users to transfer currency securely without a centralized regulator using a publicly verifiable open ledger	Zyskind, G., Nathan, O. and Pentland, A. S. (2015) 'Decentralizing privacy: Using blockchain to protect personal data', Proceedings - 2015 IEEE Security and Privacy Workshops, SPW 2015, pp. 180–184. doi: https://doi.org/10.1109/SPW.2015.27
Reliability Less Volatility	The Bitcoin market is currently very volatile and susceptible to speculative bubbles compared to other fiat currencies	Katsiampa, P. (2017) 'Volatility estimation for Bitcoin: A comparison of GARCH models', Economics Letters, 158, pp. 3–6. doi: https://doi.org/10.1016/j.econlet.2017.06.023
Regulation	The latest trends argue that Bitcoin requires regulation in order to survive as a security and become a viable form of investment and holder of value.	Burks, C. (2017). Bitcoin: Breaking Bad or Breaking Barriers? North Carolina Journal of Law & Technology, 18(5)
Security of the Exchange	BitCoin is more vulnerable to cyber-attacks than traditional currencies. Of 40 BitCoin exchanges examined and found that 18 have been closed down after cyber-attacks.	Ciaian, P., Rajcaniova, M. and Kancs, d'Artis (2016) 'The economics of BitCoin price formation', Applied Economics. Routledge, 48(19), pp. 1799–1815. doi: https://doi.org/10.1080/00036846.2015.1109038
Helpfulness Investment	Bitcoin is used as a store of value for speculative investment or savings' protection	Sas, C. and Khairuddin, I. (2017) 'Design for trust an exploration of the challenges and opportunities of Bitcoin users', Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, pp. 6499–6510. doi: https://doi.org/10.1145/3025453.3025886
Profits	The profits of informed trading in the Bitcoin market are estimated to be considerably large	Feng, Wenjun, Yiming Wang, and Zhengjun Zhang. 2018. "Informed Trading in the Bitcoin Market." Finance Research Letters 26(November 2017):63–70
Alternative Currency	Bitcoin is an alternative currency in countries with weak economic system like Venezuela	England, C. and Fratrik, C. (2018) 'Where to bitcoin?', Journal of Private Enterprise, 33(1), pp. 9–30. Available at: https://www.scopus.com/inward/record.uri?eid=2-s2.0-85042129975&partnerID=40&md5=c578b6d254b20c7a741e78eb00fcfd09.

Table 6 Pairwise Similarity value Matrix (to expresses how a attribute (keyword) semantically similar is to the other attributes)

Factors	Trust	Stability	Transfer	Profitability	Openness	Knowledge	Immutable	Regulation	Security	Investment	Decentralization	Alternative Currency
Trust	1	0.20	0.32	0.27	0.23	0.50	0.15	0.29	0.51	0.46	0.31	0.47
Stability	0.20	1	0.07	0.21	0.06	0.14	0.11	0.16	0.10	0.17	0.11	0.16
Transfer	0.32	0.07	1	0.20	0.11	0.10	0.12	0.26	0.44	0.24	0.31	0.44
Profitability	0.27	0.21	0.20	1	0.21	0.24	0.18	0.21	0.25	0.44	0.32	0.37
Openness	0.23	0.06	0.11	0.21	1	0.20	0.26	0.33	0.22	0.09	0.41	0.26
Knowledge	0.50	0.14	0.10	0.24	0.20	1	0.09	0.26	0.30	0.51	0.26	0.33
Immutable	0.15	0.11	0.12	0.18	0.26	0.09	1	0.22	0.24	0.06	0.49	0.21
Regulation	0.29	0.16	0.26	0.21	0.33	0.26	0.22	1	0.33	0.40	0.46	0.50
Security	0.51	0.10	0.44	0.25	0.22	0.30	0.24	0.33	1	0.28	0.40	0.35
Investment	0.46	0.17	0.24	0.44	0.09	0.51	0.06	0.40	0.28	1	0.26	0.53
Decentralization	0.31	0.11	0.31	0.32	0.41	0.26	0.49	0.46	0.40	0.26	1	0.49
Alternative Currency	0.47	0.16	0.44	0.37	0.26	0.33	0.21	0.50	0.35	0.53	0.49	1

References

Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., & Welten, S. (2013). Have a snack, pay with Bitcoins. *13th IEEE International Conference on Peer-to-Peer Computing, IEEE P2P 2013 - Proceedings*. https://doi.org/10.1109/P2P.2013.6688717 .

Becerra, M., & Gupta, A. (2003). Perceived trustworthiness within the organization: The moderating impact of communication frequency on Trustor and trustee effects. *INFORMS, 14*(1), 32–44.

Beck, R., Avital, M., Rossi, M., & Thatcher, J. B. (2017). Blockchain technology in business and information systems research. *Business & Information Systems Engineering, 59*(6), 381–384. https://doi.org/10.1007/s12599-017-0505-1 .

Berke, A. (2017). How safe are Blockchains? It Depends. Harvard Business School Press.

Bierer, T. (2016). Hashing it out: Problems and solutions concerning cryptocurrency used as article 9 collateral. *Journal of Law, Technology & the Internet, 7*, 79–96.

Bitcoin Forum - Statistics Center. (2019). Retrieved from https://bitcointalk.org/index.php?action=stats.

Bitcoin Garden Forum-Statistics Center. (2019). Retrieved from https://bitcoingarden.org/forum/index.php?action=stats.

Bitcoin Stack Exchange. (2019). Retrieved from https://bitcoin.stackexchange.com/questions/tagged/forum.

Bouoiyour, J., & Selmi, R. (2006). Bitcoin: A begining of a new phase? *Economics Bulletin, 36*(3), 249–351. https://doi.org/10.1177/001132550603600301 .

Brezo, F., & Bringas, P. G. (2012). Issues and Risks Associated with Cryptocurrencies such as Bitcoin. *The Second International Conference on Social Eco-Informatics,* (c), 20–26. Retrieved from http://www.thinkmind.org/index.php?view=article&articleid=sotics_2012_1_40_30101.

Cryptocurrency Talk. (2019). Retrieved from https://cryptocurrencytalk.com/.

Crytalker. (2019). Retrieved from https://cryptalker.com/bitcoin-forums/.

Dai, A. M., Olah, C., & Le, Q. V. (2015). Document Embedding with Paragraph Vectors, 1–8. Retrieved from http://arxiv.org/abs/1507.07998.

Davidson, J., & Naveed, M. (2013). *The Digital Coin Revolution-Crypto Currency-How to Make Money Online*. (E. B. Series, Ed.) (1st ed.). JD-Bix Publishing.

DeVries, P. D. (2016). An analysis of Cryptocurrency, Bitcoin, and the future. *International Journal of Business Management and Commerce*, *1(2)*. Retrieved from https://www.researchgate.net/publication/316656878_An_Analysis_of_Cryptocurrency_Bitcoin_and_the_Future.

Friedman, B., Khan, P. H., & Howe, D. C. (2000). Trust online. *Communications of the ACM, 43*(12), 34–40. https://doi.org/10.1145/355112.355120 .

Grimmelikhuijsen, S. G., & Welch, E. W. (2012). Developing and Testing a Theoretical Framework for Computer-Mediated Transparency of Local Governments. *Public Administration Review, 72*(4), 562–571. https://doi.org/10.1111/j.1540-6210.2011.02532.x.

Jarvenpaa, S. L., & Teigland, R. (2017). Trust in digital environments: from the sharing economy to decentralized autonomous organizations. *Hawaii International Conference on System Sciences,* (2017), 5812–5816.

Jarvenpaa, S. L., & Todd, P. A. (1996). Consumer reactions to electronic shopping on the world wide web. *International Journal of Electronic Commerce, 1*(2), 59–88.

Jarvenpaa, S. L., Mohlmann, M., & Teigland, R. (2019). Introduction to the Minitrack on advances in trust, identity, and trusted Systems in Technology-Mediated Environments. *Proceedings of the 52nd Hawaii International Conference on System Sciences*, (January). https://doi.org/10.24251/hicss.2019.695 .

Kaplanov, N. (2012). Nerdy money: Bitcoin, the private digital currency, and the case against its regulation. *Ssrn, 25*(1). https://doi.org/10.2139/ssrn.2115203 .

Kramer, R., & Tyler, T. (1996). Trust in Organizations: Frontiers of theory and research. SAGE Publications. https://doi.org/10.4135/9781452243610.

Lankton, N. K., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into expectation disconfirmation theory. *The Journal of Strategic Information Systems, 23*(2), 128–145. https://doi.org/10.1016/J.JSIS.2013.09.001 .

Lankton, N. K., Mcknight, D. H., & Tripp, J. (2015). Technology , Humanness , and Trust : Rethinking Trust in Technology. *Journal of the Association for Information Systems, 16*(10), 880–918.

Le, Q., & Mikolov, T. (2014). Distributed representations of sentences and documents. In *International conference on machine learning* (Vol. 31). https://doi.org/10.1145/2740908.2742760 .

Li, X., Hess, T., & Valacich, J. (2008). Why do we trust new technology? A study of initial trust formation with organizational information systems. *The Journal of Strategic Information Systems, 17*(1), 39–71.

Lindman, J., Rossi, M., & Tuunainen, V. (2017). Opportunities and risks of Blockchain technologies in payments– A research agenda. In *Proceedings of the 50th Hawaii International Conference on System Sciences* (pp. 1533–1542). https://doi.org/10.5846/stxb201304080636 .

Low, K. F. K., & Teo, E. G. S. (2017). Bitcoins and other cryptocurrencies as property? *Law. Innovation and Technology, 9*(2), 235–268. https://doi.org/10.1080/17579961.2017.1377915 .

Luna-Reyes, L. F., Cresswell, A. M., & Richardson, G. P. (2004). Knowledge and the development of interpersonal trust: a dynamic model. In Proceedings of the 37th Hawaii International Conference on System Sciences, 12 pp. https://doi.org/10.1109/hicss.2004.1265241.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Ingetrative model of organizational trust. *Academy of Management, 20*(3), 709–734.

McAllister, D. J. (2018). Affect- and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal, 38*(1), 24–59. https://doi.org/10.5465/256727 .

Mcknight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial Trust Formation in New Organizational Relationships. The Academy of Management Review, *23*(3), 473–490. Retrieved from http://www.jstor.org/stable/259290.

Mcknight, D. H., Carter, M., Thather, J. B, & Clay, P. (2011). Trust in a specific technology: An investigation of its components and measures. *ACM Transactions on Management Information Systems, 2*(12), 12–32.

Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2006). Distributed representations of words and phrases and their compositionality.

CrossRef Listing of Deleted DOIs, 1, 1–9. https://doi.org/10.1162/jmlr.2003.3.4-5.951 .

Mikolov, T., Chen, K., Corrado, G., & Dean, J. (2013). Efficient estimation of word representations in Vector Space, 1–12. Retrieved from http://arxiv.org/abs/1301.3781.

Montgomery, A. (2012). *The Dearth of Ethics and the Death of Lehman Brothers*. Retrieved from https://sevenpillarsinstitute.org/case-studies/the-dearth-of-ethics-and-the-death-of-lehman-brothers/.

Nakamoto, S. (2009a). Posts of Satoshi Nakamoto. Retrieved from https://bitcointalk.org/index.php?action=profile;u=3;sa=showPosts.

Nakamoto, S. (2009b). Summary-satoshi. Retrieved from https://bitcointalk.org/index.php?action=profile;u=3.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton: Princeton University Press.

Ostern, N. (2018). *Do you trust a trust-free technology*? Toward a trust framework model for blockchain technology. International Conference on Information Systems 2018.

Nelms, T. C., Maurer, B., Swartz, L., & Mainwaring, S. (2018). Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. Theory, Culture, & Society (Special Section: Technologies of Relational Finance).

Pavlou, P. A., & Gefen, D. (2004). Building effective online marketplaces with. *Information Systems Research, 15*(1), 37–59. https://doi.org/10.1287/isre.1040.0015 .

Pollock, D. (2018). *Is Bitcoin dying as a payment option*? Retrieved from https://cointelegraph.com/news/is-bitcoin-dying-as-a-payment-option.

Rehurek, R., & Sojka, P. (2010). *Software framework for topic modelling with large corpora*. LREC Workshop on New Challenges for NLP Frameworks, 45–50. Retrieved from http://www.muni.cz/research/publications/884893.

Rooney, K. (2018). $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. *CNBC*. Retrieved from https://www.cnbc.com/2018/06/07/1-point-1b-in-cryptocurrency-was-stolen-this-year-and-it-was-easy-to-do.html.

Ruyter, K. D., Moorman, L., & Lemmink, J. (2001). Antecedents of commitment and Trust in Customer–Supplier Relationships in high technology markets. *Industrial Marketing Management, 30*(3), 271–286.

Scott, B. (2016). How can Cryptocurrency and Blockchain technology play a role in building social and solidarity finance? *United Nations Research Institute for Social Development, 1*, 17–564. https://doi.org/10.1007/s10273-011-1262-2 .

Thatcher, J. B., McKnight, D. H., Baker, E. W., Arsal, R. E., & Roberts, N. H. (2011). The role of trust in postadoption IT exploration: An empirical examination of knowledge management systems. *IEEE Transactions on Engineering Management, 58*(1), 56–70. https://doi.org/10.1109/TEM.2009.2028320 .

Walton, J., & Dhillon, G. (2017). Understanding digital crime, trust, and control in Blockchain technologies. *Proceedings of Twenty-Third Americas Conference on Information Systems (AMCIS 2017)*, (2008), 1–10.

Woodford, I. (2019). JPMorgan launches its own cryptocurrency; the first for a major U.S. bank. Retrieved from https://www.theblockcrypto.com/2019/02/14/jp-morgan-launches-its-own-cryptocurrency-the-first-for-a-major-us-bank/.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th international congress on big data*, BigData Congress *2017*, (June), 557–564. https://doi.org/10.1109/BigDataCongress.2017.85 .