2019

Understanding the Creation of Trust in Cryptocurrencies: Bitcoin

Venkata Marella,

Bikesh Raj Upreti

Jani Merikivi

32ND BLED ECONFERENCE
HUMANIZING TECHNOLOGY FOR A SUSTAINABLE SOCIETY
JUNE 16 – 19, 2019, BLED, SLOVENIA, CONFERENCE PROCEEDINGS
A. Pucihar (ed. et al.)

University of Maribor Press

Understanding the Creation of Trust in Cryptocurrencies: Bitcoin

VENKATA MARELLA, BIKESH UPERTI & JANI MERIKIVI

Abstract Compared to traditional financial services, cryptocurrencies lack any kind of institutional, monetary, or legal backing. Yet, the popularity of the cryptocurrencies remains intact despite several adversaries. In the context of lacking basic premises as a financial tool, these cryptocurrencies provide security and earn users' trust via under-lying technologies. Despite the presence of a plethora of research in both trust and cryptocurrencies, there is a clear lack of research on what factors of the underlying technology drive trust. To uncover the factors contrib-uting to building trust, we analyzed 1.97 million discussion posts related to Bitcoin, the oldest and most widely used cryptocurrency. From the theory, we found out that functionality, reliability, and helpfulness are the con-structs to evaluate the trust in technology. Based on our analysis, we discovered 11 different factors related to three constructs of technology garnering users' trust in Bitcoins. Our results highlight factors that require atten-tion to developing new technologies that users can trust.

Keywords: • Cryptocurrency • Trust • Functionality • Reliability • Helpfulness • Bitcoin •

CORRESPONDENCE ADDRESS: Venkata Marella, Doctoral Student, Aalto University, Department of Information and Service Management, Espoo, Finland, e-mail: venka-ta.marella@aalto.fi. Bikesh Upreti, Doctoral Student, Aalto University, Department of Information and Service Management, Espoo, Finland, e-mail: bikesh.upreti@aalto.fi. Jani Merikivi, Associate Professor, Grenoble Ecole De Man-agement, Management, Technology and Strategy, Grenoble, France, e-mail: jani.merikivi@grenoble-em.com.

DOI https://doi.org/10.18690/978-961-286-280-0.44 ISBN 978-961-286-280-0
Dostopno na: http://press.um.si

1 Introduction

Trust has been and still remains a core component of financial transactions and payments. Individuals need assurance that the transactions they make are processed and completed fair and safe, a requirement that puts financial intermediaries (e.g., commercial banks) and central banks in the business of trust (Nelms, et al., 2017). These financial intermediaries guarantee the security of the customer's account and financial transactions. Customers trust these financial intermediaries and pay some amount of money as a transaction fee for their services. Unfortunately, such a trust was recently put to test due to failures in accountability and transparency due to events like the collapse of Lehman Brothers (Marella, 2017). This led individuals to look elsewhere for new alternatives, such as cryptocurrencies, which at the advent of Bitcoin in 2009, gained slow yet enduring popularity.

Cryptocurrencies (e.g., Bitcoin, Ethereum, and Ripple) are defined as digital cash where cryptography is used to ensure the security of the transactions, and to govern the supply of digital coins in circulation (Davidson & Naveed, 2014). There are three key drivers that set cryptocurrencies apart from paper monies. First, they have no central authority, and, hence they are claimed immune to government interference and manipulation. This makes them a viable alternative especially in countries with volatile currencies and unstable economies (Brett, 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 across international borders.

While technology sets individuals free from the business of trust, cryptocurrencies do not exist without evil. Further, compared to other financial tools cryptocurrencies suffer four shortcomings. First, since they are not backed up by any institution or legislation, and while this takes out the transaction fee, it also makes cryptocurrencies unpredictable, volatile, and risky (Brezo & 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 & Bringas, 2012). Third, Bitcoin and all other cryptocurrencies do not have legal status as an investment option in many countries yet. Therefore, buying or selling Bitcoins from these countries would be extremely difficult. Hence, there are several uncertainties and barriers involved with cryptocurrencies. Finally, the value of cryptocurrencies is extremely volatile for a wide variety of reasons including the cyber-attacks on the wallet (i.e., software that stores your private and public keys one needs to send and receive cryptocurrency), and exchanges (i.e., online intermediaries that help buy, sell, or exchange cryptocurrencies for other currencies).

Both the online financial services and cryptocurrencies rely on underlying technologies to secure transactions, except cryptocurrencies lacking institutional backing of central authority. The use of cryptography is driven by trust in technology in cryptocurrencies whereas traditional financial services benefit from an extra layer of trust from the institution. In the absence of basic legal and institutional premise, cryptocurrencies demand trust, not in people but in technology (Jarvenpaa & Teigland, 2017) (Ostern, 2018) as the security of financial transaction depends upon the underlying technology. The soaring popularity of cryptocurrencies implies that there are still millions of enthusiasts willing to trust in the underlying technology and try out cryptocurrencies.

Despite the wealth and diversity of research on cryptocurrencies and trust in technology (Lankton, McKnight and Thatcher, 2014), only a few studies have so far examined trust and technologies within the cryptocurrency domain ((Ostern, 2018); (Walton & Dhillon, 2017)). What is still lacking is knowledge of the attributes that add to individuals' trust in technologies (e.g., blockchain, cryptocurrency wallet, and exchanges) when they apply them for a particular purpose. That is, **what attributes of a set of technologies foster trust in a cryptocurrency domain?** Bridging this gap is of crucial importance since locus of trust is shifting from people to technology (Jarvenpaa & Teigland, 2017) (Lindman, et al., 2017). In addition, using technologies fostering the transactions of cryptocurrencies must come with low risk and uncertainty (Xin, et al., 2008). Understanding what specific attributes of technology increase trust comes thus with a managerial implication: technology designers and business professionals learn what technology attributes are most relevant to existing and potential users.

The findings are also beneficial for other domains like governance (e.g., voting and taxing) or healthcare (e.g., incorruptible medical data) where reliable technology is a must (Beck et al., 2017).

The paper unfolds 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 & McKnight, 2014). We use these constructs to better understand what develops trust around cryptocurrencies. As for empirical evidence, we focus on Bitcoin, as it is the most popular and widely used cryptocurrency (Lindman, et al., 2017). To understand how trust links to technology, we analyze 1.97 million posts extracted from a popular cryptocurrency forum (Bitcointalk.org). Our analysis of the bitcoins related posts builds on text content model employing *doc2vec,* a deep learning model for text data, proposed by Le and Mikolov (Le & Mikolov, 2014). The results report the technological features semantically closest to each of these three trust constructs. We will conclude the paper with a discussion.

2 Background

2.1 Underlying technology

Cryptocurrencies rely on three technological elements: blockchain, cryptocurrency wallets, and exchange platforms. Of these, blockchain technology is the backbone 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 the unique identifier termed 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 content of its 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 can add new blocks to the chain. The following simplified diagram represents the data structure of the blockchain.

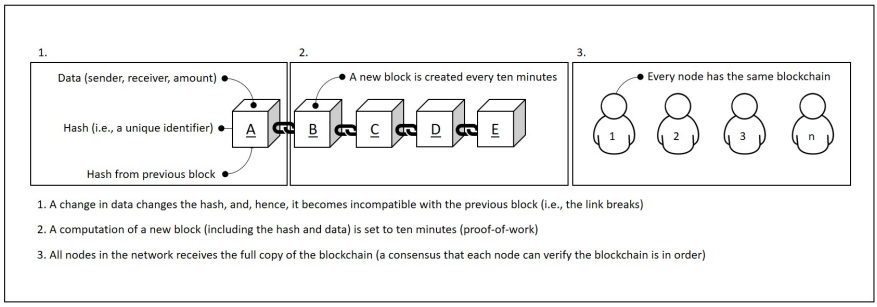

Figure 1: A simplified representation of a blockchain data structure

A Cryptocurrency wallet is a software program that stores public and private keys of the account and can interact with blockchain to enable to manage the account. These wallets make the transfer of cryptocurrencies easier (Anon., 2017). However, they are vulnerable to cyber-attacks and which cause a loss of value to the cryptocurrencies. A cryptocurrency exchange is a web-service that provides its customer's services for the exchange of cryptocurrencies into various assets such as fiat or other digital currencies (Anon., n.d.). Exchanges buy the cryptocurrencies from sellers and sell to the buyers. Some of the reputed exchanges include in Coinbase, Kraken, Bitstamp, etc. Cryptocurrency Wallets can be either stored on a hardware device, or a wallet software that can be saved either on the computer or with an exchange.

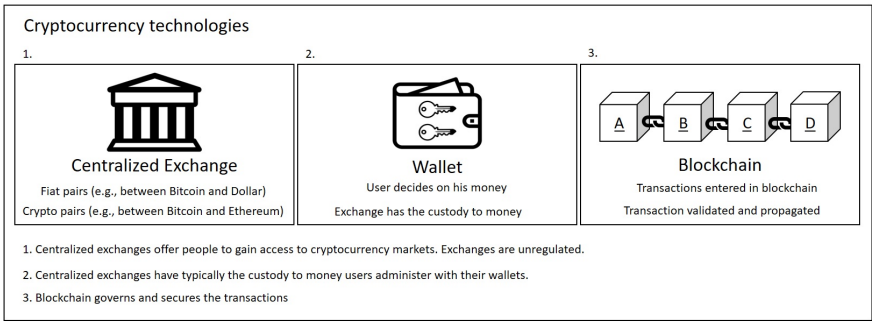

Figure 2: Cryptocurrency Technologies

2.2 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 & Davis, 1995). Trust is a dynamic concept that develops over time. Trust is an individual's reliance on another person under conditions of dependence and risk (Roderick & Tom, 1996). Reliance allows the fate of one person to be determined by another. Trustor is a person who holds certain expectations about the other party, while the trustee is a person or an entity that is assessed by the trustor (Beerra & Gupta, 2018).

While trust is studied extensively and with varying perspectives (McAllister, 1995) (Ruyter, et al., 2001), also in IS research (S. Jarvenpaa, 1997) (P.A. Pavlou, 2004), research on trust in technology is still in its infancy, yet very much demanded. McKnight et al. (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 in technology. While trust in technology excludes moral volition since technology has typically left moral conduct and decision-making to its users it seems to hold especially true when technologies, such as blockchain or other self-sufficient artifacts, eliminate the third parties. With these technologies, users have no option but to make themselves vulnerable to the capacity of technology to help achieve their goals (e.g., A smartphone user trusts that it connects well to the internet). Therefore, the question goes: "what is it about technologies that make individuals find them trustworthy?"

The current trust in technology literature employs two different types of trust constructs in technology. The first one is the 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 trusting constructs in humans, these characters would translate into helpfulness, reliability, and functionality when it comes to trusting the features of the technology. The underlying idea behind associating these trust constructs to technology is that they reveal what specific features add value (McKnight, et al., 2011). That is, if a user believes that blockchain survives from malicious attacks due to

decentralization, then it is likely that the user perceives this feature trustworthy, and, hence, valuable (Thatcher, et al., 2011).

Concerning the three trust constructs proposed by McKnight et al. (Mcknight *et al.*, 2011) and empirically validated by Lankton et al. (Lankton et al., 2014) , 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). Functionality is conceptual very similar to ability or competence. It refers to the belief that the specific technology has the capability, functions, and features, to do the required task (e.g., software that translates texts from one language to another language). Integrity is the belief that a trustee would associate with a set of principles that are acceptable to the trustor (e.g., a translator that translates texts from one language to another language during office hours). Reliability is like integrity and can be defined as the feature that technology operates consistently over a period (e.g., software that translates texts from one language to another language at all times). Benevolence is the belief that trustee has a motivation to do something good to the trustor besides being profitable (e.g., a translator who besides translating texts from one language to another language during office hours advice where to take the texts that needs be translated outside office hours). Helpfulness is like benevolence and described as the belief that technology provides adequate and responsive assistance for users via their help features (e.g., software that besides translating texts from one language to another language at all times guides on how to enable the speech recognition feature). See Table 1 for the three constructs.

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

In this study, we adopt the above three constructs and anchor them to the underlying cryptocurrency technologies (i.e., the blockchain, cryptocurrency wallet, and exchanges) described earlier in this chapter. We acknowledge that individuals intending to use or already using cryptocurrencies may have different expectations about these technologies than those using them for other purposes (i.e., features that cryptocurrency users trust in these technologies may not be the same features that actors in the music industry, who care about intellectual rights, trust in them). That is, the features these trust constructs a link to are context-dependent and this is because the uncertainty technology arises among users depend on their goals. To tap into this contextuality, we seek to identify the key trusted features with user-generated data over the years, which helps us uncover trust characterized as persistent.

3 Method

In this section, we will talk about our data collection process from the popular online Bitcoin forum. Later, we end the section by describing our model in detail.

3.1 Data Collection

Our objective is to understand how the Bitcoin earned trust from its users' despite being faceless and devoid of any legal and institutional backing. In this context, discussion forums have played a crucial role in the growth of Bitcoin, as the users engage in the discussion and interaction to share knowledge and information. Among various online discussion forums, "Bitcointalk.org" is the most popular and the oldest online forum with a large user base. We base our analysis on the bitcoin-related discussion posts collected from "Bitcointalk.org" for two important reasons. First, compared to other data sources, online discussion platform acts as a good alternative to source data as the discussions, interactions, opinion and the flow of information can be accessed on an unprecedented scale. Second, discussion data do not condition the study or experiment to be conducted but rather generated naturally by the users. This allows us to infer the technology attributes related to trust in Bitcoin from the users' own statements and words that were used to address the users' concerns or sharing 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 Bitcoins only, we limit our analysis to general discussions on Bitcoins covering 3 subtopics, such as legal, press release and legal. We downloaded about 2 million discussion posts, from March 1, 2012, to September 21, 2018 that included original posts, replies, date of the post, and the details about the users who posted.

3.2 Text modeling

Our approach requires us to identify the factors that contributed to creating trust among Bitcoin users. The first step in this direction requires us to identify the posts that relate to trust. A naïve approach would be to use a simple keyword

[1] https://pypi.org/project/beautifulsoup4/

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 in writing. Further, users can use all different combination of words to mean trust. Second, a keyword-based search for trust returned us over 10000 posts. With this large amount of search results, identify relevant posts requires manually reading all the posts which are both time and resource consuming. Moreover, ordering the post on the trust scale is a difficult task considering it requires developing a consistent and reliable rating method and overcoming the variance among the ratters. To circumvent these issues, we rely on the vector representation of word and documents generated using paragraph vector, also known as doc2vec, proposed by Le & Mikolov, 2014 (Le & Mikolov, 2014). In learning the semantic similarities, doc2vec methods have shown superior performance to competing methods ((Dai et al., 2015), (Le & Mikolov, 2014)). The root of paragraph vector method lies in the usage of the neural network to predict 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 to maximize prediction of the nearest word. However, unlike the classification problem, these networks output the learned weight as a vector as a semantic representation of text rather than the final prediction from the model. These vectors, word embeddings, are considered as the 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-art performance in learning semantic similarities and relationship. For instance, the word vector method could produce a relationship such as "Paris – France + Italy = Rome" (Mikolov et al., 2013). Later this idea was extended by Le & Mikolov, 2014 (Le & Mikolov, 2014) as a paragraph vector, also known as doc2vec that could learn the semantic representation for both the words and documents in same vector space. Their approach involved important improvements such as this method was the ability to retain word order, unlike methods like Bag of words and also allowed the text of variable length.

To train doc2vec model, we relied on implementation provided by python package "Gensim" (Rehurek & Sojka, 2010). Among available models, we trained three different variants of 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 sum. Due to the huge resource requirement in estimation PV-DM with concatenation, we omitted it from our potential model alternatives. In training models, for all three doc2vec models, we set same model parameters; the size of the vector 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. In our model, while learning the semantic relationship, our model considers 10 words at a time in a sliding fashion for each document. Given that the post can be of varying length, we consider the context window size of 10 to be a reasonable choice. Similarly, epoch refers to the number of training iteration and we train 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 and thus was our preferred choice.

Figure 3 summarizes the methodological approach used in the analysis of discussion posts collected from our 'Bitcointalk.org". Our methodology involves cleaning and pre-processing of text followed by training doc2vec model. Once the model is trained and preferred model is selected, we analyzed data building upon two sets of output from doc2vec model; a) word vectors, semantic representation of words in the collection of posts b) document vectors, semantic representation of the actual posts. To analyze the data, we first extracted fifty posts closet to the keywords related to the constructs, "reliability, functionality, and helpfulness". Given a word, the doc2vec model can return similar documents, words with similarity score using cosine similarity. The cosine similarity is computed over the vector representation of the given words and the closest word or document vectors 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 deem it's as a suitable method to extract relevant posts.

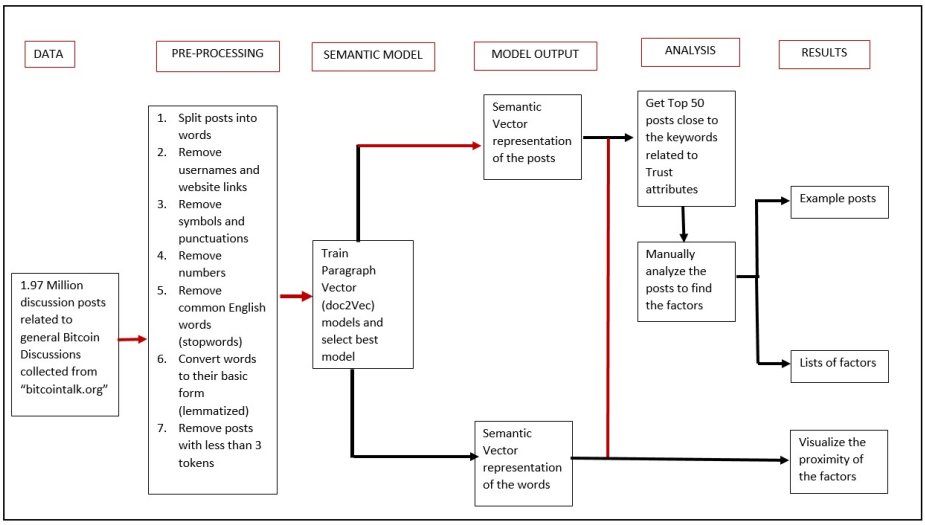

Figure 3: The Methodological approach used in the analysis of data

Once the posts are collected, we read through the posts to identify the factors from the posts. Based on identified factors we present our results in terms of a description of these factors with example posts. Additionally, we also visualize the proximity of these factors, to trust, based on the word vectors learned from the data. Since the word vectors are in 300-dimensional space, we visualize these word vectors in two-dimensional space reduced using Multi-dimensional scaling (Buja et al., 2008). The 2-dimensional plot visualizes the semantic closeness of the semantic vectors of identified factors and the semantic vector of trust.

4 Results

Our analysis is built on the output from doc2vec model of discussion posts. To identify the factors related to trust, we first extracted fifty most similar posts to the keywords related to the trust-related constructs; "Functionality", "Reliability" and "Helpfulness". The most similar posts are based on the similarity score between the word vector of the constructs and the posts. To search for the constructs, we listed our keywords that are often used about the existing technology and institutions in financial transactions. For instance, to represent the functionality, we searched for keywords such as Performance, Quick Transfer, Purchases, and Payments. Similarly, in identifying reliability related

posts, we searched for posts closest to the keywords like Stability, Regulations and knowledge. Finally, we used keywords words like Investments, Profits, and, Alternative Currency as words associated with Helpfulness construct. In total, we searched for posts related to constructs using seventeen keywords (four related to functionalities, nine for reliability and four for helpfulness) and extracted the top fifty posts for each keyword. We read through and analyzed these eight hundred fifty posts and found eleven factors relate to three constructs functionality, reliability, and helpfulness. Table 2 lists the factors as features with the description and similarity scores. Additionally, the table also links Trust factors related to functionality and reliability, to the technology/technologies that are exclusive to bitcoins and cryptocurrencies. The table links three technologies such as Blockchain technology, Cryptocurrency Wallet, and Cryptocurrency exchange to Trust related factors. Finally, we mentioned the similarity with the given keywords and the content of the post with a similarity value mentioned next to the post. Similarity value one refers that the post is completely like the keywords and a similarity value zero refers that post is not like the given keywords.

Table 2: Constructs of Trust in Technology * Similarity value expresses how semantically sim-ilar the feature (keyword) is to the words the given post contains. The closer the value is to one (1), the higher the similarity; ** B = blockchain, W = wallet, and E = exchange

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*	X		

	immutable and more and more people are joining the network to make it better." [0.54]			
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 posed 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]*

Our research findings suggest that Coin Transfers, Immutability, Openness, and Decentralization are the functional factors of Bitcoin that created 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 & Teo, 2017). Similarly, openness refers to the property that the information on the blockchain is available to the public. The feature of having a robust publicly available distributed blockchain creates trust among Bitcoin users (Berke, 2017). The Decentralized structure, Openness, and Immutability are the unique features of the Blockchain technology and are major factors contributing to trust creation among Bitcoin users.

In reliability, we found that factors like stability, regulation, security, and knowledge of Bitcoin would make Bitcoin a reliable technology. Bitcoin is often criticized for its volatility (Bouoiyour & Selmi, 2016). Users expressed concerns about the volatility in the value of Bitcoin. They strongly felt that the stability in the value of Bitcoin would make it more reliable. Secondly, contrary to a certain segment of the user's beliefs, many users believed that the regulations would make Bitcoin more reliable and convince many others to use it. According to the article written by Kaplanov in Loyola Consumer Law Review (Kaplanov, 2012), Bitcoin would flourish under legal regulation. Thirdly, 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 very reliable. Finally, users who had 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 regards to the factors related to the helpfulness of Bitcoin, many users agreed that Bitcoin was a great investment tool to earn profits in the short term. The acceptance of Bitcoin as a payment system has not completely evolved yet (Pollock, 2018). Most users consider Bitcoin 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 easily buy them. Hence, it serves as an alternative currency in those countries.

Once the factors related to trusts are identified from the posts, we also explored their semantic closeness to trust. For the purpose, we plotted word vectors of these factors with the word vector of trusts. Since the word vectors are learned from the actual data generated by the discussions among the users from the Bitcoin community, relative positions of these factors and trust help us to visualize how close or far these factors are in the actual discussion. Figure 4 plots the vector representation of the factors and trust in two-dimensional space vector space obtained by applying Multi-Dimensional Scaling (MDS) (Buja et al., 2008). The figure shows that openness and immutable, the unique functionality of bitcoin, are closer to the trust. This proximity implies that in the bitcoin-related discussions these unique functionalities, among all factors are closely associated with trust. Further, factors related to profit and transfers are close to each other whereas factors like regulation, security and stability are close to each other. Deviating from our expectation, the Decentralized structure as a factor of trust remain further away from all factors including trust.

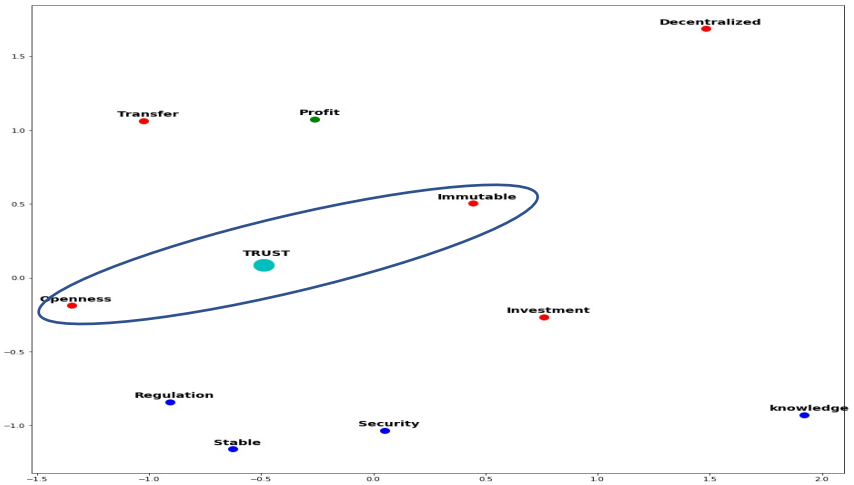

Figure 4: Semantic proximities among Trust and the associated factors

5 Discussions and Conclusion

In this study, we aimed at examining trust in technology within the cryptocurrency domain. To do this, we employed the technology trust model proposed by Lankton et al. (Lankton et al., 2014) and focused on three distinct trust constructs: functionality, reliability, and helpfulness. We then used them to identify the specific features, which contribute to trust in technologies (i.e., the blockchain, cryptocurrency wallet, and exchanges) that underlie cryptocurrencies. As for the empirical analysis, we decided to focus on Bitcoin, because it is currently 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 we performed draws on a paragraph vector model termed doc2vec (Le and Mikolov, 2014), which produces a semantical representation of words and posts. This allowed us to map the semantically most relevant features to the three trust constructs.

The results suggest that trust is semantically closest to the unique features offered by blockchain technology. The features raised in the posts are ledger immutability and openness, the former securing safe and fair transactions, and the latter making the transactions accessible to the public. Immutability refers 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 and hence making the system completely transparent. Openness creates transparency while Immutability creates accountability. Transparency is considered as the key elements to create a trust (Grimmelikhuijsen, et al., 2013). These two functionalities are the unique features offered by cryptocurrencies using Blockchain technology. The degree of transparency and accountability offered by Bitcoin or other cryptocurrencies is unparalleled to any financial institution across the world including the investment banker Lehman Brothers. These unique technological attributes made the Bitcoin users to trust Bitcoin even without any backing or support from any institution.

Our research makes three important contributions to the literature related to Trust in cryptocurrencies. First, we add uniqueness of technology as a construct that contribute to the trust in technology model. Secondly, we combine large-scale data from the Bitcoin community with state-of-art textual analysis as-as research methodology for studying the factors that create trust in technology. Finally, the research results can be generalized to the literature related to building trust in new products that rely highly on technologies and automation. For example, the driverless car, to win users' trust.

Our data for the research is collected from Bitcointalk.org online forum, which is the oldest online forums on Bitcoin. However, the forum consists of a wide category of users, which includes users who are not Bitcoin users. Hence, the trust factors that we identified from the textual analysis is not exclusive to the opinions of the actual Bitcoin users. Further, Bitcoin users outside of this forum are not included in our analysis. The paper can be extended further by including the user-level analysis into the research.

References

Beck, R. A., Rossi, M., & Jason, T. (2017). Blockchain Technology in Business and Information Systems Research. Business & Information Systems Engineering, 59(6), 381–384.

Beck, R., Czepluch, J., Lollike, N., & Malone, S. (2016). BLOCKCHAIN-THE GATEWAY TO TRUST-FREE CRYPTOGRAPHIC TRANSACTIONS. Association for Information Systems.

Beerra, M., & Gupta, A. (2018). Perceived Trustworthiness within the Organization: The Moderating Impact of Communication Frequency on Trustor and Trustee Effects. INFORMS.

Berke, A. (2017, March 07). How Safe Are Blockchains? It Depends. Harvard Business Review.

Blockgeeks . (2017). Retrieved from https://blockgeeks.com/guides/cryptocurrency-wallet-guide/

Bouoiyour, J., & Selmi, R. (2016). Bitcoin: a beginning of a new phase? Economics Bulletin, 36(3), 1430-1440.

Brett, S. (2016). How can cryptocurrency and blockchain technology play a role in building social and solidarity finance?

Brezo, F., & Bringas, P. (2012). Issues and Risks Associated with Cryptocurrencies such as Bitcoin. International Conference on Social Eco-Informatics.

Buja, A., Swayne, D., Littman, M., Dean, N., Hofmann, H., & Chen, L. (2008). Data visualization with multidimensional scaling. Journal of Computational and Graphical Statistics. Journal of Computational and Graphical Statistics, 17(2), 444-472.

Christopher, C. M. (2016). THE BRIDGING MODEL: EXPLORING THE ROLES OF TRUST AND ENFORCEMENT IN BANKING, BITCOIN, AND THE BLOCKCHAIN. NEVADA LAW JOURNAL, 17, 139.

CoinMarketCap. (2018). Retrieved August 01, 2018, from https://coinmarketcap.com/

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

Davidson, J., & Naveed, M. (2014). The Digital Coin Revolution - Crypto Currency - How to Make Money Online (JD-Biz Corp Publishing ed.). Entrepreneur Books.

Doney, P. M., & Cannon, J. P. (1997). An Examination of the Nature of Trust in Buyer - Seller Relationships. Journal of Marketing;, 61(2), 35.

Grimmelikhuijsen, S., Im, T., Porumbescu, G., & Hong, B. (2013). The Effect of Transparency on Trust in Government: A Cross-National Comparative Experiment. Public Administration Review, 73(4), 575-586.

Hosein, N. (2009). Internet Banking: An Empirical Study Of Adoption Rates Among Midwest Community Banks. Journal of Business & Economics Research, 7(11), 51-72.

Iansiti, M., & Lakhani, K. (2017). The truth about Blockchain. Harvard Business Review(January and February).

Investopedia. (2019). Retrieved from https://www.investopedia.com/terms/b/bitcoin-exchange.asp

Jeffrey, S. (2015). Bitcoin and modern alchemy: in code we trust. Journal of Financial Crime, 156-169.

Kaplanov, N. (2012). Nerdy Money: Bitcoin, the Private Digital Curency, and the Case Against. Loyola Consumer Law Review, 25(1).

King, M. (2004). The Institutions of Monetary Policy. San Diego: American Economic Association.

Lankton, N., McKnight, D. H., & Thatcher, J. B. (2014). Incorporating trust-in-technology into Expectation Disconfirmation Theory. Journal of Strategic Information Systems, 23(2), 128-145.

Lankton, N., 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. (pp. 1188-1196). International Conference on Machine Learning .
Lindman, J., Rossi, M., & Tuunainen, V. (2017). Opportunities and risks of Blockchain. Hawaii International Conference on System Sciences .
Low, K., & Teo, E. (2017). Bitcons and other cryptocurrencies as property? Law, Innovation, and Technology, 9(2), 235-268.
Luther, W. J. (2015). CRYPTOCURRENCIES, NETWORK EFFECTS, AND SWITCHING COSTS. Contemporary Economic Policy.
Marella, V. (2017). Bitcoin: A Social Movement Under Attack. Association for Information Systems.
Mayer, R., & Davis, J. (1995). An Integrative Model Of Organizational Trust. Academy of Management Review, 20(3), 709-734.
McAllister, D. J. (1995). Affect- and Cognition-Based Trust as Foundations for Interpersonal Cooperation in Organizations. Academy of Management, 38(1), 24-59.
McKnight, H., Carter, M., Thatcher, J., & Clay, P. (2011). Trust in a Specific Technology: An Investigation of Its Components and Measures. ACM Transactions on Management Information Systems, 2(2).
Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., & & Dean, J. (2013). Distributed Representations of Words and Phrases and their Compositionality. (pp. 3111-3119). NIPS Proceedings.
Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System.
Narayanan, A., Bonneau, Joseph Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies (1st ed.). Princeton University Press.
Nelms, T. C., Maurer, B., Swartz, L., & Mainwaring, S. (2017). Social Payments: Innovation, Trust, Bitcoin, and the Sharing Economy. Theory, Culture, & Society(Special Section: Technologies of Relational Finance).
P.A. Pavlou, D. G. (2004). Building effective online marketplaces with institution-based trust. Information Systems Research, 15((1)), 37-59.
Pollock, D. (2018). Is Bitcoin Dying as a Payment Option? . Retrieved January 12, 2018, 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. In P. o. Frameworks. (Ed.)., (pp. 45--50).
Roderick, M. K., & Tom, R. T. (1996). Trust in Organizations. Business & Economics.
Rooney, K. (2018). $1.1 billion in cryptocurrency has been stolen this year, and it was apparently easy to do. Retrieved June 07, 2018, 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., Luci, M., & Jos, L. (2001). Antecedents of Commitment and Trust in Customer–Supplier Relationships in High Technology Markets. Industrial Marketing Management, 30(3), 271-286.
S. Jarvenpaa, P. T. (1997). Consumer reactions to electronic shopping on the World Wide Web. International Journal of Electronic Commerce, 1(2), 59-88.
S.X. Komiak, I. B. (2006). The effects of personalization and familiarity on trust and adoption of recommendation agents. MIS Quarterly, 30(4), 941-960.
Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How The Technology Behind Bitcoin Is Changing Money . Penguin UK.

Thatcher, J., McKnight, H., Baker, E., Arsal, R., & Robert, N. (2011). The Role of Trust in Postadoption IT Exploration: An Empirical Examination of Knowledge Management Systems. IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT, 58(1).

White, L. H. (2014). The Market for Cryptocurrencies. CATO, 35(2), 383.

Xin, L., 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.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data (BigData Congress), 557-564.