2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Society (ICSE-SEIS)

Trust beyond computation alone: Human aspects of trust in blockchain technologies

Barnaby Craggs
Department of Computer Science
University of Bristol
Bristol, United Kingdom
barney.craggs@bristol.ac.uk

Awais Rashid
Department of Computer Science
University of Bristol
Bristol, United Kingdom
awais.rashid@bristol.ac.uk

***Abstract*—Blockchains – with their inherent properties of transaction transparency, distributed consensus, immutability and cryptographic verifiability – are increasingly seen as a means to underpin innovative products and services in a range of sectors from finance through to energy and healthcare. Discussions, too often, make assertions that the trustless nature of blockchain technologies enables and actively promotes their suitability—there being no need to trust third parties or centralised control. Yet humans need to be able to trust systems, and others with whom the system enables transactions. In this paper, we highlight that understanding this need for trust is critical for the development of blockchain-based systems.**

Through an online study with 125 users of the most well-known of blockchain based systems – the cryptocurrency Bitcoin – we uncover that human and institutional aspects of trust are pervasive. Our analysis highlights that, when designing future blockchain-based technologies, we ought to not only consider computational trust but also the wider eco-system, how trust plays a part in users engaging/disengaging with such eco-systems and where design choices impact upon trust. From this, we distill a set of guidelines for software engineers developing blockchain-based systems for societal applications.

***Keywords*-Blockchain, Trust, Bitcoin, Guidelines**

I. Introduction

It is not uncommon to hear discussions of how blockchains will revolutionize everything from banking to security in the Internet of Things (IoT), from the press to government, often with the presumption that the transparency of an accessible ledger will promote, engender or increase trust in the applicable industry. By design, blockchains are distributed throughout peers in a network with whom validation of new records (or blocks) is required before they are added to the *public* chain. When a new block is added it contains a hash – a unique fingerprint – of the previous block. Each new addition, therefore, being immutable, cannot be changed. In addition to being distributed, blockchains have a decentralized governance model meaning that no single party can approve additions to the chain, nor can they make unilateral changes to the technology of blockchain.

It is this combination of architectural design choices, and the distributed and decentralized nature which differentiates blockchain-based systems from more classically centralized systems, and consequently leads many to believing that blockchains present a potential silver-bullet for a range of societal applications from finance and energy to healthcare and open government, e.g., [1]–[5].

Whilst it may be the case that blockchain will revolutionize these sectors, it is *highly* unlikely that unless people trust implementations that they will be adopted, be used, provide stakeholder returns or engender loyalty [6]—let alone deliver on those original promises.

As yet there are limited real-world, and successful, implementations [7] from which we can understand how humans will trust such solutions. One area in which blockchains are well understood is that of crypto-currency. Whilst it seems a new crypto-currency appears every week, Bitcoin[1] provides a prototypical use-case for blockchain within which the impact of design decisions upon trust can be explored. This, in turn, can guide design choices for other blockchain-based systems so that they account for, engender and facilitate human trust.

We studied a group of 125 Bitcoin users, as a proxy for users of blockchain-based systems, and found prevalent expressions of interpersonal trust. The novel contributions of our work are:

- Clear evidence that, despite traditional viewpoints of the trust in blockchain being solely in computation, trust in other people is a critical concern for users.
- Discussion of how trust can be impacted positively (and negatively) by the technical choices made in the design and maintenance of Bitcoin.
- Design guidelines that articulate how these aspects of trust will occur, and need to be accounted for, in the design of future blockchain-based systems and applications.

The rest of this paper is structured as follows. Section II provides background on literature on interpersonal trust and the need to study such notions in the context of blockchain-based systems. Section III offers an overview of Bitcoin as the prototypical (and most widely deployed) blockchain and discusses whether *trustless* is a term truly applicable to such an eco-system. Sections IV and V, respectively, describe the study methodology and the measures & constructs used to

[1]***Nomenclature.*** Based upon community norms, the uppercase form 'Bitcoin,' is used to refer to the Bitcoin ecosystem including the protocol. A lowercase 'b' written as 'bitcoin' is usually associated specifically with bitcoin as the currency.

978-1-7281-1762-1/19/$31.00 ©2019 IEEE
DOI 10.1109/ICSE-SEIS.2019.00011

analyze trust. Section VI discusses aspects of interpersonal trust uncovered by our study while Section VII highlights the impact of loss upon trust. Section VIII reflects on two of our guidelines following the Bitfinex hack that occurred after the completion of our study. Section IX contrasts our study with related work and Section X concludes the paper and identifies directions for future work.

II. Background: Interpersonal trust

Trust is often defined as being empirically based and probabilistic: "*to a degree consistent with our perception of the available evidence. In human interaction, we trust individuals and institutions to the degree that they have, over time, proved trustworthy*" [8]. Similarly, Mayer *et al* [9] argue that any such trust is cyclically developed based upon the trustor's perception of the other party and their own propensity to trust, and that without both factors trust cannot exist. Thusly, trust is contextual to the trusting party.

Trust also lies at the core of almost all theories of interpersonal relationships [10]. There are few aspects of life within which trust does not play an indispensable role – trust pervades human society [11], [12]. Kramer and Carnevale [13] argue that trust involves a set of beliefs and expectations that another's actions will be in some way beneficial to long term self-interest; a position that could only be established were the trustor able to cognitively assess another person's (or organization's) actions from an empathetic perspective.

Within a blockchain an emergent notion of trustlessness comes from its practical use as a pseudonymous peer-to-peer based network. Once a transaction has been logged within the blockchain it is known to everyone, in the network, that it has been concluded. Consequently, there is no need to trust, or even know, who a counter-party is when transacting.

However this view is problematic in that it only caters for the payment side of a transaction and in no way affords guarantee that the goods or services being purchased will actually be delivered. That is still utterly dependent upon trust or third party assurity [14]. This, in turn, requires institutional trust from the users, which may be underpinned by a form of centralized control, such as regulation [6]. With people needing to mitigate risk by placing trust in something beyond computation alone, services like escrow and smart contracts built around the blockchain fill the void – and incidentally also act as as explicit statements of mistrust within which precise terms for an expectation of service and remedial action are articulated for the avoidance of doubt.

It follows that, as new uses emerge for blockchain technologies, the ecosystem is evolving not to remove centrality or the need to trust a governing institution but rather to cater for a very human need to be able to understand and remove risk in everyday life – to be able to see certainty in outcomes.

III. Bitcoin - A Prototypical Blockchain

Conceptually Bitcoin was a product of its time. By the late 2000s intrusive organizational demands for personal data were being recognized and world economies were in the early stages of incredible decline. The indiscretions of financial institutions were laid bare for all to see and it was apparent that a great many people were going to suffer loss in the years to come. Mistrust of the handling of this crisis by financial institutions, central banks and governments was growing. In a period of such uncertainty and, arguably, fear it was very easy to view this as being an opportunity for an alternative approach to the hitherto centrally regulated payment channels.

Whilst Riegelsberger *et al* [15] argue that systems should promote trustworthy behavior, when first proposed—as an alternative payments system—the intention for Bitcoin was to remove the need for trust altogether. Trust, in these parties, was viewed as a necessary evil in traditional economics, borne out of the need to mitigate inherent risks where bad actors exist in a system. Nakamoto argued that this was leading to organizations "*hassling*" customers for "*more information than they would otherwise need*", the implication being that this was in some way a form of risk mitigation against customer's potentially fraudulent behaviors.

By design, Bitcoin is intended to be trustworthy by actually being *trustless* in those very persons or organizations that one may mistrust.

The term *trustless* was coined by an early adopter community with a converged world-view and, for many in and around Bitcoin, this purist view of *trustless* remains, i.e., the trust model for payments is "*based in computation rather than people*" [16]. But Bitcoin has evolved beyond payments alone, into a more socio-technical ecosystem; new use cases have emerged (e.g., investment speculation, gambling, laundering, digital asset signing, etc.) and the community around it has grown. And organizations, decentralized or not, including mining pools, exchanges, wallet providers and product/service vendors all need trust in order to cooperate, negotiate and transact [17].

Truly Trustless? The crypto-trust that underpins Bitcoin is essential in securing the whole ecosystem but, in this evolved environment it seems a little narrow to view Bitcoin as being totally *trustless*. Not least as with all technologies relied upon to secure assets (informational or otherwise), people (i.e., software engineers) are responsible for design, implementation and operation of these technological tools. As Lacey [18] points out "*despite the presence of advanced technical controls, information systems remain vulnerable because of human behavior*" – something which Bitcoin's inception was designed to actively mitigate against and is being discussed as a prime reason for adopting blockchain. Yet cases of miscreant and inadvertent detrimental behavior within Bitcoin abound.

IV. Study Methodology

Our on-line study sought to understand if and in whom bitcoin users placed trust, contrary to the trustless nature of Bitcoin itself. The study was reviewed and approved by the relevant institutional research ethics committee. It was widely advertised to a number of Bitcoin and research-participant related on-line forums, websites, social media and also through

Source	n	Has Used	Purchase or Sale	Transfer funds	Launder money	Investment	Drive adoption	Other	Study or Research
Reddit	97	77	67	54	2	57	35	6	5
Internal	8	3	2	1	-	1	-	-	1
Twitter	7	3	3	3	-	3	2	-	-
BitCoinTalk	5	5	5	3	1	5	4	-	-
Unknown	5	4	3	3	-	1	-	1	1
Email	1	1	-	-	-	-	-	1	-
Facebook	1	-	-	-	-	-	-	-	-
StackExchange	1	1	1	1	-	-	1	-	-
Total	125	94	81	65	3	67	42	8	7

TABLE I: Bitcoin usage by survey respondent source

direct email asking for voluntary participation with no offer of payment. A summary of the main sources of respondents, and their own personal uses of bitcoin, can be seen in Table I.

The study asked a number of questions[2] looking at:

1) participant demographics,
2) personality type,
3) discovery and use of the crypto-currency,
4) general sentiment towards Bitcoin and its long-term prospects, and
5) loss events.

These questions allowed us to examine aspects of trust within Bitcoin, in particular looking for interpersonal trust in other users and those developing / maintaining bitcoin, institutional trust in the exchanges being used to trade bitcoin, and technological trust in Bitcoin itself. From these we can draw insights as to how design decisions, for other blockchain-based technologies, may impact on user trust.

A. Demographics

In total 181 responded to the invitation with fifty-six excluded from the analysis for either not having completed the questionnaire or for bogus participation, such as making offensive or spam comments in response to open ended questions. Respondents were allowed to only participate once (enforced by client-side cookie and server-side IP registration) with the ability to take the study in stages over a maximum of five days in total.

Of the qualified responses (N=125), overwhelmingly 88% of respondents were male. Sixty-seven percent of all respondents considered themselves *'employed'* with another 26% *'still in education.'* Eighty-eight percent were located in either Europe (n = 68) or the Americas (North & South) (n = 42).

B. Bitcoin

Exposure to Bitcoin amongst respondents peaked in 2012-2013 with 86% having heard of Bitcoin prior to the collapse in pricing of early 2014. Amongst respondents, on-line discussion forums provided first exposure for 43%, with friends/family member/colleagues and on-line news websites accounting for another 41%. Ninety-four (94) respondents expressed how they have or are using Bitcoin. Of those: purchasing or selling things was the most prevalent use (86%) followed by investment/speculation (71%).

Whilst only 9% of the 125 respondents agreed that Bitcoin was primarily being used for criminal activity, 36% felt theft was hampering Bitcoin's adoption. Three respondents admitted to having used Bitcoin to launder money themselves.

V. Measures & Constructs

A. Interpersonal Trust

We directly extracted each respondent's levels of interpersonal trust in other Bitcoin users (T_U) and the people maintaining Bitcoin (T_D) – each determined through a single five-point Likert response and represented in Figure 1.

B. Propensity to trust

The NEO Personality Inventory (NEO-PI-R) [19] looks to define the "*Big Five*" personality domains of neuroticism, extraversion, openness to experience, agreeableness and conscientiousness. Taken together, the five domains with their underlying thirty facets (or sub-traits) are viewed as a "*comprehensive and detailed assessment of normal adult personality.*" Within this study we look to the domain of *agreeableness* which is a personality trait where a low score relates to selfish behaviors and lack of empathy. Congruent with Lucassen & Schraagen [20] we do not apply the full NEO-PI-R questionnaire as other traits (and sub-traits) are not relevant to this study, choosing to only apply sub-trait questions for propensity to trust. Respondents answered 8 questions (see Appendix) as to how much they felt the statements applied to themselves, with the total sum of results being used to assign a score to the respondent (T_P). The construct T_P allows us to approximate whether levels of both interpersonal or information trust may be the result of this underlying personality type.

C. Sentiment towards Bitcoin

Sentiment towards Bitcoin was measured using 6 questions (see Appendix) about aspects of Bitcoin: price rises, adoption, regulation, viability as a currency, investment potential and criminal activity. The total sum of results was used to assign a sentiment score to the respondent (S). The construct S allows us to approximate whether a respondent's underlying sentiment (positive or negative) to Bitcoin might influence interpersonal or information trust ratings.

A summary of constructs (T_P & S) can be seen in Table II.

D. Construct Validity

For the two constructs (T_P & S), questions used a five-point Likert scale where 1 = 'strongly disagree' and 5 = 'strongly agree'. Cronbach's Alpha (α) was used to test the internal reliability of each construct. As a function of the number of items in a test, it measures the co-variance between item-pairs in a construct and the variance of the total score, and is a commonly used statistical method for estimating the reliability

[2]A condensed copy of the study questions can be found in the Appendix

of a psychometric test. As such α can be viewed as the expected correlation that tests measure the same construct. For example the construct T_P had 8 questions, each being an item. In psychometric testing, common "*rule-of-thumb*" minimum acceptable requirements for internal reliability are $\alpha \geq 0.7$. Respondent's propensity to trust (T_P) had a Cronbach's α of 0.81 indicating good reliability in the questions as an indicator of trust. Sentiment (S) had a Cronbach's α of 0.70 indicating acceptable reliability.

E. Influence Upon Constructs

Overall, respondents were moderately trusting in general (*mean = 27, standard deviation = 5.1*) with a positive sentiment towards Bitcoin (*mean = 21, standard deviation = 4.3*). Testing for statistical dependence between these constructs and when the respondent discovered Bitcoin was assessed using Pearson's Chi Squared tests. This determines the statistical likelihood of any observed difference between two categorical sets might be to chance. Simply, Pearson's Chi Squared tests whether when a respondent discovered Bitcoin impacts upon their sentiment (S) towards Bitcoin. Slightly surprisingly, no significant relationship to S was observed, meaning that how long a respondent had known about Bitcoin was not influencing their sentiment.

VI. Evidence of Interpersonal Trust

A. Trust in other users (T_U)

The common view of Bitcoin is that its model of trust lays solely within computation - that there is no need to trust people. Overall, across the 125 respondents, trust in other users (T_U) was just below neutral (*mean T_U = 2.928, standard deviation = 0.805*) indicating a very slight mistrust in others, which thusly does not seem particularly surprising.

However, participants were more than willing to express notions of interpersonal trust in other users of Bitcoin. Given this seeming disparity with doctrine, we looked to whether a respondent's propensity to trust (T_P) or their sentiment towards Bitcoin itself might be influencing that slight mistrust. A visual inspection of the influence of respondent's personal propensity to trust (T_P) and sentiment towards Bitcoin (S) upon their trust in other users can be seen in Figure 1 A & B. From this it actually appears that, whilst the mean response is slightly mistrusting, actually trust in other people increases with both underlying personality traits and their sentiment towards Bitcoin.

Using ordinal logistic regression we tested the null hypothesis that neither T_P or S had no influence, and found that only sentiment could be shown to significantly influence trust in other users of Bitcoin at a 95% confidence level. This is a surprising finding as one might well expect a positive sentiment to follow doctrine and decrease trust.

B. Trust in people (software engineers) maintaining Bitcoin (T_D)

Whilst the distributed team of developers charged with the ongoing maintenance and upkeep of Bitcoin (the core development team) can be argued to form an *organization* with centralized control [21], [22], respondents (rightly) still viewed this group as people and expressed trust there also. This can be seen in Figure 1 C & D. Unlike users, we had expected to find respondents more trusting of the developers. Especially as they can only act with agreement and so a form of peer consensus could be also viewed as a precursor for them being viewed as trustworthy. This was initially confirmed with trust in developers (T_D) being above neutral indicating a slight trust (*mean T_D = 3.064, standard deviation = 0.905*). Unlike user trust, using ordinal logistic regression, we found that trust in developers was significantly influenced by both propensity to trust and sentiment – more so when combined.

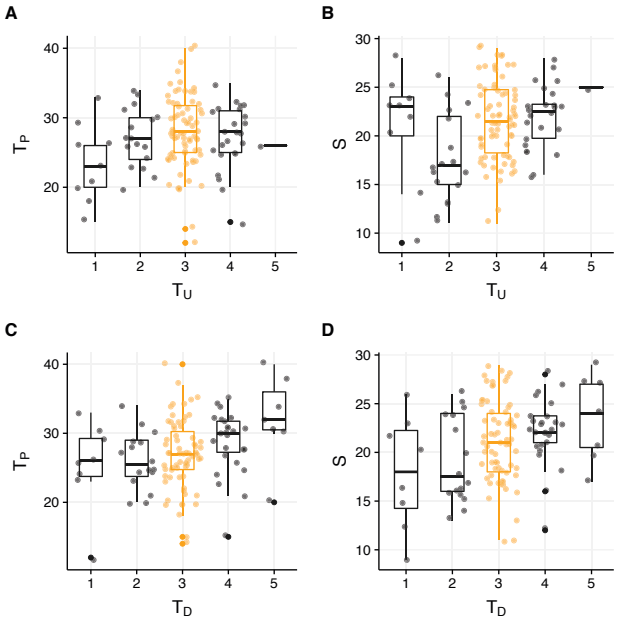


Fig. 1: Trust in people (T_U & T_D) against Trust propensity (T_P) and Sentiment (S)

Guideline #1 - Interpersonal Trust Impacts on Adoption

Given that, even within a slightly mistrusting Bitcoin community, interpersonal trust is still prevalent we would expect the same to be true of any blockchain implementation. Whilst it may be that trust in other users may not be a prime concern, trust in those building and maintaining such solutions will be—a position supported by Zarifis *et al* [17] in that a user's "*level of trust in a technology is an important factor in the level of its adoption*".

C. Trust is Dependent

Using a manual open-coding approach to classify respondents' reasons for how and why they rated their trust in other people using Bitcoin, we identified that user

	Propensity for Trust (T_P)		Sentiment towards Bitcoin (S)	
Category	Score	%	Score	%
Very high	36-40	3.2%	26-30	15.2%
High	31-35	24.8%	21-25	44.0%
Moderate / Neutral	20-30	68.0%	16-20	32.0%
Low	13-19	3.2%	11-15	8.0%
Very Low	8-12	0.8%	6-10	0.8%
		100% (N=125)		100% (N=125)
Mean score	T_P = 27, SD = 5.1 (category = moderate)		S = 21, SD = 4.3 (category = positive)	

TABLE II: Summary of constructs

behavior was a critical factor in trusting/mistrusting other users.

Context - A number of respondents did allude to interpersonal trust being context specific. For example, trusting a *'bricks and mortar'* vendor selling books for small amounts of bitcoin might require a different assessment of trust compared to, say, a person peddling drugs on a Dark Web marketplace.

Sentiment - The role of sentiment towards Bitcoin appears to be critical in how respondents assess other people. It is unclear as to why this might be the case although there is perhaps a key difference in the roles that *'other users'* and *'people maintaining Bitcoin'* play – especially in terms of interaction with respondents.

As respondents (in the majority) were also users of bitcoin it is likely they had had numerous cyclical interactions in similar contexts (multiple discussions across different forums for example) with *'other users'*—sufficient to generate trust judgments. The same is not necessarily true of interactions with '*people maintaining Bitcoin.*' This core development team is generally well known throughout the Bitcoin community with members regularly being called upon by news agencies and conferences to pass comment or judgment on various crypto-currency aspects. But these *one-way* interactions (i.e., the respondent is consuming information from a core development person) are different to that of the *two-way* interactions within an active discussion.

So whilst trust in *'other users'* may be linked to those prior interactions, it seems plausible (given the critical role the core development team play in maintaining Bitcoin) that a positive sentiment towards Bitcoin (S) may be acting as some form of proxy for that missing interaction when making judgment on what are a distant non-interacting party.

Mistrust - A little over 25% of reasons related to the behavior of other users, particularly behaviors that might be either criminal or in some way manipulative. The behaviors of other users (e.g., fraud, theft or market manipulation) were cited by several respondents as rationale for trust judgments – in the main mistrust. It is unclear from the data collected if these judgments were based on single, perceived, vicarious or repeated (cyclical) experiences. Respondents citing behavior did exhibit slightly below average scores for trust in other users (T_U) and a slightly negative sentiment (S) and it is possible these contribute to the rationale. Without specifically asking for qualification from respondents, this is conjecture. That said, with behavior of others applied as a rationale for trust this reinforces that interpersonal trust is evident in Bitcoin.

Guideline #2 - Interpersonal Trust Will Provide Resilience Against Loss of Trust Through Errant Behavior

It is almost impossible to use technology to mitigate human behaviors, especially those that might be in some way subversive or adversarial. What is clear is that perceptions of negative behavior on the part of others impact trust. We would expect that where trust in those building and maintaining the blockchain can be engendered – perhaps through ongoing engagement with user groups – then trust in blockchain-based systems and services is likely to be more resilient to the inevitable miscreant events they will endure.

VII. The Impact of Loss Upon Trust

Amongst all the stories of fantastical price rises are almost as many tales of people losing bitcoin. From the unfortunate loss of a hard-drive containing 7,500 bitcoins in late 2013 to a landfill site [23] through to the widely publicized collapse of the exchange Mt.Gox in early 2014, most likely from the alledged theft of 600-800,000 bitcoin.

Such losses impact upon trust. Of the respondents who claimed to have or being using Bitcoin (N = 94), 62.4% felt they have incurred a loss of Bitcoin (see Table III). Forty-five respondents gave details as to how they had lost bitcoin and rated on a five point Likert scale how this loss had impacted upon their interpersonal trust in Bitcoin users (T_U) and, in the people maintaining Bitcoin (T_D). The impacts of loss (*mean T_U = 2.689 & mean T_D = 2.911*) both indicated that interpersonal trust was slightly reduced when losing Bitcoin.

Moving slightly away from interpersonal trust briefly; we also looked at whether loss impacts upon a general trust in Bitcoin (T_B) and, in Bitcoin exchanges (T_E). Whilst loss had no mean impact upon trust in Bitcoin (*mean T_B = 3.000*) there was a more marked reduction in trust of the exchanges (*mean T_E = 2.489*).

When we look at individual types of loss we can see a more nuanced impact with trust being, in the main, negatively

		*Mean Impact on Trust After Loss**				*Significant Impacts Upon Party*			
Reason for Loss	n	T_U	T_D	T_B	T_E	Party	ChiSq (x^2)	DF	p
Fraud	18	2.444	3.000	3.056	2.222	-	-	-	-
Exchange Collapse	18	2.778	2.778	2.833	1.889	T_E	24.058	3	0.000
Rate Variations	12	2.583	2.667	2.667	2.167	T_E	7.878	3	0.049
User Error	11	2.727	3.091	3.273	3.000	T_E	12.419	3	0.006
Theft	8	2.375	2.750	2.875	1.875	T_U	7.805	3	0.050
						T_E	7.879	3	0.049
Exchange Problems	5	2.600	2.400	2.400	1.600	T_D	9.056	3	0.029
						T_E	13.715	3	0.003
						T_B	9.562	4	0.048
Other	4	2.750	2.750	3.000	3.000	-	-	-	-
Gambling	2	3.500	3.500	3.500	3.000	T_U	22.213	3	0.000
						T_B	10.334	4	0.035

*(Notes: *where 1="much lower" 2="lower" 3="about same" 4="higher" 5="much higher")*

TABLE III: Impacts of loss upon trust

impacted by loss. Interpersonal trust (T_U) is most negatively impacted by fraud and theft events. Non-interpersonal trust tends to remain reasonably stable. However, trust in exchanges (T_E) suffers markedly through both technical problems at exchanges (mean of 1.600 indicating *much lower / lower*) and collapse of an exchange (mean of 1.889 indicating *lower*). Interestingly trust in the people maintaining Bitcoin (T_D) was most negatively impacted by loss from technical problems at exchanges, something for which they have no direct, and little (if any) indirect responsibility.

Pearson's Chi-Squared tests of impact of loss (by reason) against these four parties show significant results—the most notable being T_E being pegged to the collapse of exchanges, and T_U being pegged to gambling.

A. Gamblers trust more

Whilst gambling is fully related to T_U, it appears that loss from gambling actually increases trust across all four parties. Some caution is applied to this finding as this context sample size was only two — however we posit that, as an often repeated behavior, gambling actually fulfills the cyclical pattern of interactions. A key issue in trusting within gambling is fairness. If one player has lost, but s/he does not suspect the game is rigged or the other party is cheating, any loss would not likely reduce their trust, as some loss is an essential element of gambling and thus expected. Further the acceptance of bitcoin as a payment method on gambling websites may demonstrate a desirable level of technical prowess which, when combined with a consistency in aspects such as reliable payment of winnings, helps to engender or even bolster trust.

B. Fraud does not reduce trust in Bitcoin, but theft does

Finally there are notable differences in impact between fraud and theft events. Both are behaviors undertaken by other parties but it appears respondents view them differently. For example, fraud has negligible impact upon T_D & T_B and its greatest impact upon T_E. For theft the impact is across the board, again with the most pronounced being upon T_E. In both cases it appears that other users might be perceived to be to blame for the loss and that exchanges may in fact shoulder greater blame (again perhaps these reports pertain to the huge losses incurred by many in early 2014). The lack of impact on T_D & T_B through fraud appears to suggest that theses parties are not viewed as being at fault, however the same is not true in theft events – something that may hint at concerns about underlying security issues in Bitcoin.

C. Self enacted loss can increase trust

Where respondents were able to attribute loss to their own failings (user error) it reduced T_U, the reasons for which are unclear. A common theme for 'user error' was lost wallets, keys or passwords. An increase in T_D & T_B might be linked to this personal error reinforcing underpinning concepts of security within Bitcoin wallets.

An equally plausible scenario is based in economic fundamentals which dictates how the relationship between supply and demand will impact upon price. For example, as supply in oil decreases, given a stable demand, the price will increase. Conversely a drop in demand and increase in supply will drop prices. For anyone with a belief in these fundamentals and knowing there is limited supply of bitcoin (the hard limit of 21 million), any loss of bitcoin would result in the value of retained bitcoin actually increasing—a process which would reinforce foundational notions of decentralization and (institutional) trustlessness.

Two key areas of system design that directly impact upon user trust related to the loss of bitcoin are: *transaction confirmation* and *pseudonymity*. It is all but impossible to reverse erroneous transactions in Bitcoin. This is a result of the design choice to not mandate multi-signatory transactions (which are facilitated by the protocols) where at least two of the confirmations are made by the transacting parties and the casting vote is made by a third party in the event of disagreement. As confirmations are left open to peers on the network, confirmations are blind to transaction fulfillment, and the loss of bitcoin due to fraudulent or theft events is permanent. Further, the pseudonomity afforded in Bitcoin means that attempts to recover losses via mechanisms such as legal action are at best unlikely.

Guideline #3 - Protocol Choices can Both Improve and Degrade Trust

In future blockchain implementations, understanding how properties of the protocol can lead to unintentional consequence will be critical, not just for user trust and adoption, but also long term viability. Attempts to facilitate removal of, or even thwart erroneous blocks being written to the blockchain (possibly through alternative consensus mechanisms such as proof-of-stake [24]) need to be considered not just for their technical capability but also how such mechanisms might be perceived and trusted/mis-trusted by users.

D. Exchange collapses impact all aspects of trust

Thusly, it should come as no surprise that trust in exchanges, people and Bitcoin itself is impacted negatively by loss events. In an ecosystem where loss through fraud and theft is widely publicized, the knowledge that the transfer of one's bitcoins is one-way is perceived as a huge trust issue by potential users, with potential to hamper mainstream adoption.

Trust in exchanges (T_E) suffers the most as a result of technical problems or a collapse of the exchange itself. Given the high profile collapse of Mt Gox in early 2014 and the widespread technical problems it and other exchanges endured in the weeks prior, this is not surprising. The more interesting insight is these technical problems or collapses negatively impact all four measured areas T_U, T_D, T_B and T_E.

Guideline #4 - Highly Visible Failures Impact Everyone

It is perhaps facile to point out that nobody wants their implementation of a blockchain-based system to fail. It is fair though to envisage multiple competing offerings in the early stages as with crypto-currencies in general. But what designers should understand is that when one system fails, all systems are tarred with the same brush—everyone is subject to a dent in how much users trust the more generic technology. Expecting, and even planning, for how to react to such events should be standard practice. One possible solution lays within *Guideline #2* above, in more fully engaging with user communities so that strengthened interpersonal trust of those behind the technology helps to mitigate the wider impact of failure upon trust.

VIII. Post-study Reflection of Bitfinex Hack

A. The breach

On August, 2nd 2016 Bitfinex — the largest (by volume) exchange at the time — was hacked [25], resulting in a loss of ∼US$70M worth of bitcoin and being the largest single loss since the collapse of MT Gox in 2014. As news broke, the velocity of the already falling price of bitcoin increased, with closing prices having fallen ∼17% to under US$500. In the immediate aftermath press coverage was largely negative with many predicting another full exchange collapse. However Bitfinex, recognising the potential impact of the negative press in conjunction with significant financial loss, reacted swiftly and released almost daily press announcements about the event.

B. The response

On August, 6th Bitfinex posted details of a recovery plan in which losses would be generalized (socialized) across all depositors - a 36.067% 'haircut' - by way of a $1 bond-like security ('BFX' token) for later redemption, "*we are crediting a token labelled BFX to record each customer's discrete losses. Tokens will be distributed without release or waiver. The BFX tokens will remain outstanding until redeemed in full by Bitfinex or possibly exchanged upon the creditor's request and Bitfinex's acceptance for shares of iFinex Inc.*" [26]. This was a clear indication by Bitfinex, and their parent company iFinex, that they not only intended to keep trading but also to make good on those losses, and could readily be interpreted as an exercise in re-building customer and market trust.

The announcements updating customers, now creditors, continued over the following weeks, detailing how breach investigations were proceeding, how BFX redemptions were being made and when tokens were being converted at scale into equity as promised.

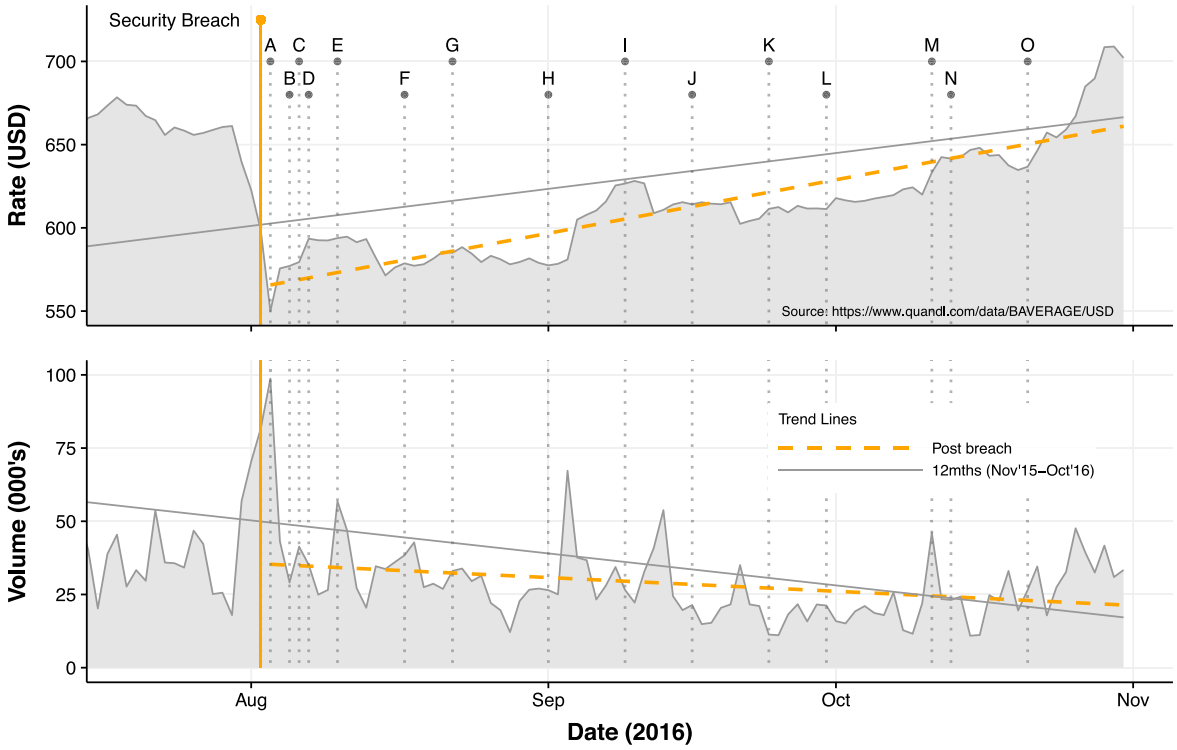
C. The 'effect'

Exactly how users viewed this breach is unclear. For some the attack may have been viewed as theft, decreasing interpersonal trust. For others, Bitfinex may have been viewed as institutionally untrustworthy. For some it is possible that as the underlying protocols were not overtly viewed as being at fault and trust in Bitcoin itself might have actually increased. What is likely from this study's findings is that trust will have been impacted across all parties (T_U, T_D, T_B & T_E). In all cases, however, this supports this study's view that the trust model of Bitcoin—as an evolving ecosystem—goes beyond computation alone.

Given this, the efforts by Bitfinex to restore confidence seem well placed, and support *Guidelines #2 & #4*. A visual inspection of average bitcoin pricing [27] across multiple exchanges (as this flattens out the more direct impact on Bitfinex-only pricing) shows that post-breach the velocity of price rises actually increased, and the decline in volume eased (see Figure 2). Whilst Bitfinex's actions cannot be proven to be causal — without both statistical and user confirmation — when the timings of their announcements are superimposed (with the exception of A,F & H) each was followed within a day by a rise in price, albeit a slight one. Announcements F & H also pre-date similar rises but with greater lag of approximately 2 to 3 days.

IX. Related Work

Existing research on blockchain technologies predominantly focuses on Bitcoin and on four key streams therein.



Bitfinex 2016 Breach Announcements (https://www.bitfinex.com/posts)

A – Security Breach – Update 1
B – Security Breach – Update 2
C – Security Breach – Update 3
D – Site Relaunch
E – Platform Service Update
F – Interim Update
G – Bitfinex signs letter of intent with BnkToTheFuture
H – Redemption of 1.1812% of BFX Tokens
I – BFX Token–for–Equity Exchange Details Imminent
J – Special Purpose Vehicle (SPV) Opportunities
K – BFX token to iFinex equity conversion update
L – Redemption of 1.3152% of BFX Tokens
M – RRT Exchange Trading Enabled
N – Bitfinex Announces Sizable Token–for–Equity Exchange by Customers
O – Message to the individual responsible for the security incident of 2nd Aug 2016

Fig. 2: Impact of Bitfinex security breach and subsequent recovery efforts on bitcoin markets

The *first stream* looks at the technology and its functionality of the currency and its protocols e.g., [17], [28], [29]. The *second stream* studies the security, privacy and stability of the wider Bitcoin ecosystem, e.g., [21], [30]–[33]. The *third stream* considers economic, e.g., [34]–[39] and governance, e.g., [40]–[43] factors. The *fourth stream*, more recently and adjunct to Bitcoin, looks at alternative uses (primarily) for blockchains or distributed ledger technology (DLT) as it is becoming known, e.g., [44]–[46].

Work examining the human dimensions of trust and how they impact the adoption and usage of blockchains is limited. Maurer, Nelms & Swartz [47] attribute social (interpersonal) trust to the distributed nature of peers and code that underpin Bitcoin. Lustig & Nardi [48] and Christoper [41] explore the nature of trust in the algorithms. Zarifis *et al* [17] build a model for transactional trust within business to consumer relationships. Works by Sas and Khairuddin [49]–[51], through small-scale user studies, explore user perceptions and trust from a Human Computer Interactions (HCI) perspective and acknowledge the "*lack of empirical work exploring the experience of using Bitcoin and the issues of trust surrounding it.*"

Thusly, understanding human behavior – and more specifically concepts of trust (as is the focus of this paper) – helps shape the software engineering community's understanding of the main barriers to mass adoption of blockchain-based systems. This understanding is critical to the design, implementation and maintenance choices being made, as well as the impacts of loss events and media exposure upon user perceptions and sentiments towards that system. This also bears close relationship to the emerging body of work on values in software engineering [52], [53]; user trust is a key *value* in blockchain-based systems that are being proposed for delivery of critical services such as finance, energy and healthcare.

X. Conclusions

It is with no small irony that, despite Nakamoto's intention to remove the need for trust in third-parties [54], Bitcoin is replete with interpersonal trust. Indeed, without such trust it is impossible to envisage how Bitcoin could have achieved its meteoric rise, nor how other implementations of blockchain will be adopted let alone be sustainable or achieve their promise. This study has highlighted perceptions of interpersonal trust

within the Bitcoin ecosystem, how events such as loss can impact trust and how design decisions can not only facilitate that loss but also be harnessed to mitigate against potential mistrust. Whilst we acknowledge that such trust is both context and application dependent, given the commonality of the underlying blockchain technology, we expect similar aspects of interpersonal trust to be significant within future implementations of blockchain.

With this in mind, design choices being made at the time of development of similar socio-technical systems are likely to have consequences upon the trust that users have in those systems—the less a user finds a system trustworthy, the less likely they are to adopt and use it. Based on our study of Bitcoin as the prototypical blockchain, we have distilled four guidelines for design of blockchain based system and design considerations that can help engender trust and hence adoption.

Our study is a first step towards understanding *in whom, why and how trust is placed by users* of blockchain-based systems as an active part of the functional requirements definition in an effort to facilitate adoption. Further research is needed on other large-scale blockchain-based systems as they emerge to validate, refine and extend our proposed guidelines. Research is also needed to probe key properties of the blockchain implementation – for example, the choice of consensus protocol – to measure the impact upon user trust, and, in turn impact upon ongoing participation.

Overall we conclude that *trustless* is a loaded term not well understood and often misinterpreted to mean that there is no notion of trust in blockchain-based systems. Whilst at their core, such systems may rely upon computation for trust, the day to day operation is dependent upon human aspects of trust that software engineers must take into account during the design of such systems.

ACKNOWLEDGEMENTS.

This work has been funded by the UK Engineering and Physical Science Research Council (EPSRC) as part of PETRAS: Cybersecurity of the Internet of Things Research Hub (grant no EP/N023234/1), the HighWire post-disciplinary Doctoral Training Centre (grant no EP/G037582/1), and HoSEM: Household-Supplier Energy Market (grant no EP/P031838/1).

REFERENCES

[1] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Transactions on Dependable and Secure Computing*, 2016.

[2] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Computer Science-Research and Development*, vol. 33, no. 1-2, pp. 207–214, 2018.

[3] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," *Journal of medical systems*, vol. 40, no. 10, p. 218, 2016.

[4] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.

[5] S. Ølnes, "Beyond bitcoin enabling smart government using blockchain technology," in *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 2016, pp. 253–264.

[6] V. Shankar, G. L. Urban, and F. Sultan, "Online trust: a stakeholder perspective, concepts, implications, and future directions," *The Journal of Strategic Information Systems*, vol. 11, no. 3, pp. 325 – 344, 2002. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0963868702000227

[7] M. Higginson, M-C. Nadeau, and K. Rajgopal, "McKinsey Report - Blockchain's Occam problem," https://www.mckinsey.com/industries/financial-services/our-insights/blockchains-occam-problem, [Last Accessed 01-Feb-19].

[8] J. Evensky, "Adam smiths's essentials: On trust, faith, and free markets," *Journal of the History of Economic Thought*, vol. 33, no. 02, pp. 249–267, 2011.

[9] R. C. Mayer, J. H. Davis, and F. D. Schoorman, "An integrative model of organizational trust," *Academy of Management Review*, vol. 20, no. 3, pp. 709–734, 1995.

[10] J. A. Simpson, "Psychological foundations of trust," *Current Directions in Psychological Science*, vol. 16, no. 5, pp. 264–268, 2007.

[11] J. S. Coleman, *Foundations of Social Theory*. Harvard University Press, 1994.

[12] N. Luhmann, *Trust and Power*. Wiley, 1979.

[13] R. M. Kramer and P. J. Carnevale, *Trust and Intergroup Negotiation*. Blackwell Publishing Ltd, 1998, pp. 431 – 450.

[14] I. Flechais, J. Riegelsberger, and M. A. Sasse, "Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems," in *Proceedings of the 2005 Workshop on New Security Paradigms*. ACM, 2005, pp. 33–41.

[15] J. Riegelsberger, M. A. Sasse, and J. D. McCarthy, "The mechanics of trust: A framework for research and design," *International Journal of Human-Computer Studies*, vol. 62, no. 3, pp. 381 – 422, 2005. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S1071581905000121

[16] A. Antonopoulos, "Bitcoin security model: trust by computation," 2014, [Last Accessed Mar-18]. [Online]. Available: http://radar.oreilly.com/2014/02/bitcoin-security-model-trust-by-computation.html

[17] A. Zarifis, X. Cheng, S. Dimitriou, and L. Efthymiou, "Trust in digital currency enabled transactions model," in *The 9th Mediterranean Conference on Information Systems (MCIS'15)*, vol. 9, 2015, pp. 363–370. [Online]. Available: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1034&context=mcis2015

[18] D. Lacey, *Managing the Human Factor in Information Security: How to win over staff and influence business managers*. John Wiley & Sons, 2011.

[19] P. T. Costa and R. R. McCrae, *Professional manual: revised NEO personality inventory (NEO-PI-R) and NEO five-factor inventory (NEO-FFI)*. Psychological Assessment Resources, 1992.

[20] T. Lucassen and J. M. Schraagen, "Propensity to trust and the influence of source and medium cues in credibility evaluation," *Journal of Information Science*, vol. 38, no. 6, pp. 566–577, 2012.

[21] A. Gervais, G. Karame, S. Capkun, and V. Capkun, "Is bitcoin a decentralized currency?" *2014 IEEE Symposium on Security and Privacy*, vol. 12, no. 3, pp. 54–60, 2014.

[22] J. Matonis, "The bitcoin mining arms race: Ghash. io and the 51% issue," 2014. [Online]. Available: https://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/

[23] British Broadcasting Corporation, "Quest for lost hard drive with £4m stored bitcoins," [Last accessed: Dec 2017]. [Online]. Available: http://www.bbc.co.uk/news/av/technology-25138627/quest-for-lost-hard-drive-with-4m-stored-bitcoins

[24] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Annual International Cryptology Conference*. Springer, 2017, pp. 357–388.

[25] Bitfinex, "Announcements," 2016, [Last accessed: Dec-16]. [Online]. Available: https://bitfinex.com/posts

[26] Bitfinex, "Security breach - update 3," 2016, [Last accessed: Dec-16]. [Online]. Available: https://www.bitfinex.com/posts/129

[27] Quandl, "Usdbtc weighted aggregate price," [Accessed: Dec-16]. [Online]. Available: https://www.quandl.com/data/BAVERAGE/USD-USD-BITCOIN-Weighted-Price

[28] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, "Sok: Research perspectives and challenges for bitcoin and cryptocurrencies," in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121.

[29] F. R. Velde, "Bitcoin - a primer," *Chicago Fed Letter*, vol. Dec, p. 317, 2013. [Online]. Available: http://www.chicagofed.org/digital_assets/publications/chicago_fed_letter/2013/cfldecember2013_317.pdf

[30] M. Bastiaan, "Preventing the 51%-attack: a stochastic analysis of two phase proof of work in bitcoin," in *22nd Twente Student Conference on IT*. University of Twente, 2015. [Online]. Available: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-of-two-phase-proof-of-work-in-bitcoin.pdf
[31] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*. IEEE, 2017, pp. 375–392.
[32] E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser, and B. Ford, "Enhancing bitcoin security and performance with strong consistency via collective signing," in *25th USENIX Security Symposium (USENIX Security 16)*. USENIX Association, 2016, pp. 279–296. [Online]. Available: https://arxiv.org/abs/1602.06997
[33] S. Meiklejohn and C. Orlandi, "Privacy-enhancing overlays in bitcoin," in *International Conference on Financial Cryptography and Data Security*. Springer, 2015, pp. 127–141.
[34] R. Böhme, N. Christin, B. Edelman, and T. Moore, "Bitcoin: Economics, technology, and governance," *The Journal of Economic Perspectives*, vol. 29, no. 2, pp. 213–238, 2015.
[35] J. Bukovina and M. Martiček, "Sentiment and bitcoin volatility," *MENDELU Working Papers in Business and Economics*, 2016. [Online]. Available: ftp://ftp.mendelu.cz/RePEc/men/wpaper/58_2016.pdf
[36] E.-T. Cheah and J. Fry, "Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin," *Economics Letters*, vol. 130, pp. 32–36, 2015.
[37] L. Kristoufek, "What are the main drivers of the bitcoin price? evidence from wavelet coherence analysis." *PLoS ONE*, vol. 10, no. 4, p. e0123923, 2015.
[38] C. Pavel, R. Miroslava, and K. d'Artis, "The economics of bitcoin price formation," *Applied Economics*, vol. 48, no. 19, pp. 1799–1815, 2014.
[39] M. Polasik, A. Piotrowska, T. P. Wisniewski, R. Kotkowski, and G. Lightfoot, "Price fluctuations and the use of bitcoin: An empirical inquiry," *International Journal of Electronic Commerce*, vol. 20, no. 1, pp. 9–49, 2015.
[40] J. Bohr and M. Bashir, "Who uses bitcoin? an exploration of the bitcoin community," in *Twelfth Annual International Conference on Privacy, Security and Trust (PST'14)*. IEEE, 2014, pp. 94–101.
[41] C. M. Christopher, "Why on earth to people use bitcoin," *Business & Bankruptcy Law Journal*, 2014. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2470628
[42] D. Garcia, C. J. Tessone, P. Mavrodiev, and N. Perony, "The digital traces of bubbles: feedback cycles between socio-economic signals in the bitcoin economy," *Journal of The Royal Society Interface*, vol. 11, no. 99, p. 20140623, 2014.
[43] R. Viglione, "Does governance have a role in pricing? cross-country evidence from bitcoin markets," *Self-published*, 2015.
[44] G. Danezis and S. Meiklejohn, "Centrally banked cryptocurrencies," in *Network and Distributed System Security Symposium (NDSS '16)*, 2016.
[45] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symposium on Security and Privacy*, 2015, pp. 839–858.
[46] S. K. Shukla, "Editorial: Cyber security, iot, block chains-risks and opportunities," *Transactions on Embedded Computing Systems (TECS)*, vol. 16, no. 3, p. 62, 2017.
[47] B. Maurer, T. C. Nelms, and L. Swartz, "When perhaps the real problem is money itself!: the practical materiality of bitcoin," *Social Semiotics*, vol. 23, no. 2, pp. 261–277, 2013.
[48] C. Lustig and B. Nardi, "Algorithmic authority: The case of bitcoin," in *48th Hawaii International Conference on System Sciences (HICSS'15)*, 2015, pp. 743–752.
[49] C. Sas and I. E. Khairuddin, "Exploring trust in bitcoin technology: a framework for hci research," in *Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction*. ACM, 2015, pp. 338–342.
[50] I. E. Khairuddin, C. Sas, S. Clinch, and N. Davies, "Exploring motivations for bitcoin technology usage," in *CHI'16 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2016, pp. 2872–2878.
[51] C. Sas and I. E. Khairuddin, "Design for trust: An exploration of the challenges and opportunities of bitcoin users," in *CHI'17 Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2017, pp. 6499–6510.
[52] B. S. Barn, R. Barn, and F. Raimondi, "On the role of value sensitive concerns in software engineering practice," in *37th IEEE/ACM International Conference on Software Engineering, ICSE 2015, Florence, Italy, May 16-24, 2015, Volume 2*, 2015, pp. 497–500.
[53] M. A. Ferrario, W. Simm, S. Forshaw, A. Gradinar, M. T. Smith, and I. C. Smith, "Values-first SE: research principles in practice," in *Proceedings of the 38th International Conference on Software Engineering, ICSE 2016, Austin, TX, USA, May 14-22, 2016 - Companion Volume*, 2016, pp. 553–562.
[54] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

APPENDIX
ABRIDGED SURVEY QUESTIONS

Construct: Propensity to Trust - NEO-PI-R

- Regarding the intentions of others I am rather cynical and sceptical
- I believe that you will be used by most people if you allow them to
- I believe that most people have good intentions
- I believe that most people with whom I have dealings are honest and trustworthy
- I become distrustful when someone does me a favour
- My first reaction is to trust people
- I tend to assume the best of others
- I have a good deal of trust in human nature

Construct: Sentiment Towards Bitcoin

- Long term (3 years +) bitcoin prices will always rise
- Long term adoption by retailers will be good for Bitcoin
- Governments will regulate Bitcoin
- Bitcoin provides a viable alternative to traditional fiat (currency)
- Long term bitcoin offers a better financial return (as an investment) than stocks
- Bitcoin is primarily a tool for criminal activity

Demographics

1) Where in the world do you Live?
2) Is English your primary language?
3) What is your primary language?
4) How good do you consider your English to be?
5) How old are you?
6) Which gender do you most identify yourself with?
7) Is this the same gender you had at birth?
8) Please indicate the highest level of education completed.
9) Employment - Do you see yourself primarily as...

Bitcoin (Condensed Format)

1) Roughly, when did you first hear about Bitcoin?
2) Can you remember from where you first heard about Bitcoin?
3) How much do you agree with the following statements about Bitcoin? (includes sentiment towards Bitcoin responses)
4) How well do these statements describe you? (includes self-rated expertise in Bitcoin responses)
5) What have you used bitcoin for?
6) Can you rank your uses of bitcoin in order of importance to you?
7) You said you have used bitcoin for investment / speculation; what position do you currently have?
8) Have you ever lost bitcoin? How?
9) Thinking about when you lost bitcoin, did this affect your trust?