Design for Trust: An Exploration of the Challenges and Opportunities of Bitcoin Users

Corina Sas
Lancaster University
Lancaster, UK
corina@comp.lancs.ac.uk

Irni Eliana Khairuddin
Universiti Teknologi MARA
Selangor, Malaysia
irnieliana@salam.uitm.edu.my

ABSTRACT
Bitcoin is a cryptocurrency which has received increasing interest over the last five years. Built upon a decentralized peer to peer system, it supports transparent, fast, cost effective, and irreversible transactions, without the need for trusting third party financial institutions. We know however little about people's motivation and experience with bitcoin currency. This paper reports on interviews with 20 bitcoin users in Malaysia about their experience and trust challenges. Findings show that bitcoins are used more as store of value for speculative investment or savings' protection. The paper advances the HCI theories on trust by identifying main bitcoin characteristics and their impact on trust, such as decentralization, unregulation, embedded expertise, and reputation, as well as transactions' transparency, low cost, and easiness to complete. We discuss insecure transactions, the risk of dishonest traders and its mitigating strategies. The paper concludes with design implications including support for the transparency of two-way transactions, tools for materializing trust, and tools for supporting reversible transactions.

Author Keywords
Bitcoin users; blockchain; trust; dishonest traders; risks.

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION

Bitcoin is a special form of alternative currency: a digital cryptocurrency described as the first open and decentralized currency [23], whose transactions are recorded on an open source, and publicly distributed ledger. This blockchain technology allows for secure and transparent transactions, while protecting the identity of transaction's parties [39]. On the one hand, such an innovative form of financial transaction appears particularly appealing to bitcoin users.

CHI 2017, May 06-11, 2017, Denver, CO, USA
 ISBN 978-1-4503-4655-9/17/05…$15.00
DOI: http://dx.doi.org/10.1145/3025453.3025886

Figure 1: Merchant's sign for accepting bitcoin payment

For example, in a preliminary study, Khairuddin and Sas [26] interviewed 9 users and identified three motivations for bitcoin use: the role of bitcoin technology in a monetary revolution, users' increased empowerment due to the open, decentralized and unregulated technology, and their perception of the increasing value of bitcoins. On the other hand, blockchain's characteristics as a decentralized and pseudo-anonymous platform can pose important trust challenges to bitcoin users such as illicit use and cyberattacks [15,53]. We argue that because of these characteristics, blockchain offers a unique case study for the exploration of trust. This contrasts with most HCI models of trust which have been informed by empirical work on e-commerce or e-payment systems which are traditionally centralized, regulated, and non-anonymous. Hence the feasibility of these models for theorizing about users' trust in bitcoin requires exploration.

Since its beginning in 2009, blockchain technology has steered increasing research interest predominantly in the areas of cryptography, security, and peer to peer computing. Relevant HCI work has just started to emerge [5,26,43]. We still know little about bitcoin users and their experience or how different blockchain's characteristics impact on trust. This paper addresses this gap, by reporting on interviews with 20 bitcoin users about their motivations and experience of using bitcoins and their trust related issues. We addressed the following research questions:

- Which are the *motives* for early adoption and use of bitcoins? How do people *learn* about bitcoin and how do they *use* bitcoins for?
- How different *blockchains' characteristics* impact on the various dimensions of *trust*?
- Which are the main trust *challenges* and how do people attempt to *mitigate* them?

The main contributions of this work include advancing the theoretical discourse of trust in HCI, by extending it to unregulated, decentralized and pseudo-anonymous systems such as blockchain. We also identified three design implications for supporting users' trust.

RELATED WORK

While the topic of trust has been well researched by various disciplines, for our work we selected theories developed in HCI, particularly for e-payment and e-commerce.

Trust in HCI

We agree with the definition of trust as the willingness to be vulnerable [13]. In HCI there are two main directions of conceptualizing trust: trust between people and technology, and trust between people interacting with technology. Specific HCI work exploring people's trust in bitcoin technology is just starting to emerge. For example, in their framework for exploring the trust challenges of bitcoin technology, Sas and Khairuddin [43] identified three dimensions of trust: technological (users' trust in bitcoin technology), social (trust between and among bitcoin's stakeholders: users, miners, exchanges and merchants), and institutional trust (government trust in bitcoin technology).

Two prevalent HCI models are the model of online trust [13], and the framework on mechanics of trust [41]. Corritore and colleagues [13] identified three trust factors including users' perception of technology's credibility, ease of use, and risk. Their four dimensions of credibility include honesty (well intention, truthful and unbiased actions), expertise (knowledge, experience and competence), predictability (expectation that technology will act consistently based on past experience), and reputation (recognized past performance). The model has been extensively applied to web design in e-government, e-commerce, and e-banking, but its value for blockchain technology has received limited attention. The model also shares similarities with Davis' [16] emphasis on usefulness and ease of use in his technology acceptance model.

The framework on mechanics of trust [41] investigates technology-mediated trust between users and has been applied to e-commerce. This framework identifies two key properties warranting trust in transaction's partner: *contextual and intrinsic properties*. Contextual properties are described as temporal, social and institutional embeddedness. *Temporal embeddedness* refers to parties' potential for engaging in future transactions, and interest in their relationship's longevity. This in turn prevents the risk of defection, as the present gains come at the cost of future lost ones. Temporal embeddedness requires traceability of action through "repeated interaction with stable identities" [p9, 41] so that the trustor can accumulate more knowledge and make better predictions about the trustee's future behavior. *Social embeddedness* captures the exchange of information among trustors about trustees' past performance. This motivates the trustee to fulfil the agreement in order to protect his reputation among the larger pool of trustors accessing information about his past performances. *Institutional embeddedness* captures the legal aspects underpinning transactions, able to enforce sanctions such as litigation or punishment for the parties who do not fulfil their agreement. Given this protection by the law institutions, the trustors are comfortable to engage in transactions with trustors of whom they know little.

Intrinsic properties of the trustee include his *ability* or motivation to act in a trustworthy manner inferable on the basis of his credibility; *internalized norms* which capture trustee's integrity or respect for moral principles which can be supported by the parties' social identify and presence; and *benevolence* capturing trustee's concern for the wellbeing of the other [41]. Benevolence resembles Hardin's theory of trust [24] and the *encapsulated interest:* parties' interest in relationship which tends to be rich and ongoing. He also discusses risk as the uncertainty of trustee's choice to engage in betrayal or deflection; risk which is better mitigated in group or *thick relationships* where trustee's reputation is socially embedded.

To summarize, HCI models of trust identified key factors impacting on users' trust in technology or in each other during technology-mediated transactions. There is however limited work on investigating the feasibility of these models for the exploration of trust in bitcoin technology.

Alternative Crypto Currency

Historically, people created objects as medium of exchange to replace the barter system [45]. Such objects include shells, stones or anything valuable to both buyer and seller. The argument of the medium of exchange was later extended in the 17th century through fiat money [17]: coins of precious metals issued and declared valuable by the king. Such coins were commonly deposited with goldsmiths for safekeeping, and in return, the owners were given receipts called goldsmith's notes [51]. The goldsmith role was later taken on by the government institutions issuing fiat money through their treasuries or central banks, so that nowadays the national fiat currencies are the dominant medium of exchange for trading goods or services. They also serve the role of storing value for future purchase, and of units of account in which goods and services could be priced. Over the last five centuries however, alternative medium of exchange have also emerged as substitute to national fiat currencies [21], mostly for supporting local economies and their communities [20]. Developed privately, most of the alternative currencies have no legal tender and are not regulated by national governments [28]. Alternative currencies have also emerged as unregulated digital currencies issued and controlled by developers, and used by members of virtual communities [18].

Bitcoin Technology

A more recent development of alternative currencies is crypto currencies built through cryptographic algorithms. Among the over 500 cryptocurrencies available in the current market [12], bitcoin is one of the most popular ones.

Designed by Nakamoto, an anonymous entity, bitcoin is underpinned by the blockchain technology [39] which has received increased interest from both the financial and industrial sectors [50]. The blockchain consists of a ledger distributed throughout a peer to peer network of nodes which record each transaction after it has been approved. Transactions in blockchain are represented as single data structures and from user's perspective they involve three key components: the address where the bitcoins are stored; the private key owned by the user to send bitcoins; and the wallet software, which runs on user's personal computer, used to receive, send or store bitcoins [47]. Each bitcoin transaction is created by the wallet software and broadcasted to the network where it is tested for validity and included in the blockchain.

Unlike in the banking system, the blockchain ledger is not maintained by a central authority and the verification of transactions is not ensured by trusted third parties. Instead transactions are verified and authorized by miners using secure crypto algorithms [15] ensuring thus core security functions [4]. A negative consequence of this unregulation is the feud between governments and blockchain, with some central institutions having failed to recognize its legality [49]. Previous work has also identified some scamming cyber threats faced by the bitcoin users such as scams related to fake website, ponzi scheme, phishing, and application plugin [53]. As the ledger is public, blockchain is also known as a transparent system: each machine connected to the blockchain can download a full copy of the ledger, allowing for browsing or querying the global history of transactions as well as the remaining balance of the bitcoins left in each wallet address [47]. Since it no longer requires trust in third party entities to keep the ledger, blockchain technology has been called trustless.

In Nakamoto's view [39] the concepts of irreversible transactions and trust are strongly coupled. The blockchain aims to address the key weakness of the traditional trust based model where financial institutions act as trusted third parties to mediate e-payments. Bank transactions however are costly both in time and fees. They can also be reversed by the banks, in order to arbitrate disputes between the trading parties. The problem however is that the banks are not bound to enforce the contract between the trading parties, so that refunds may be approved even if the contract stipulates otherwise. In contrast, blockchain was intended to eliminate this middle link and its higher cost, as well as the option of reversing transactions.

Another important aspect of the blockchain is protecting the privacy of the parties involved in bitcoin transactions [39]. A similar functionality is available in the banking system where the privacy is ensured by limiting access to transaction information to the involved parties and the bank. However, the protection of privacy in blockchain is even stronger, since it does not require any personally identifiable information in order to allow users to engage in bitcoin transactions. This makes the blockchain pseudo-anonymous [4]: the wallet address is public while the identity of its owner is not [39]. It is however users' responsibility to ensure that the two are never linked [15]. To support this, Nakamoto suggested the use of new wallet address for each transaction [39]. The pseudo-anonymous nature of blockchain technology lets it open to misuse on the online black market such as Silk Road, with negative consequences for blockchain's reputation [15].

To conclude, the technology underpinning bitcoin transactions has been purposefully designed as decentralized and secure, unregulated and transparent yet pseudo-anonymous. These unique strengths of the blockchain also relate to some trust challenges such as illicit use or damaged reputation. There are however limited empirical studies exploring the relationship between blockchain's properties and users' trust [30,33].

METHOD

We recruited 20 bitcoin users, 18 male, 2 female, (mean age 30, range 21-50). Six participants had less than 6 months experience of using bitcoins, 8 participants have between 6 months and 2 years, while the remaining 6 have more than 2 years. In terms of educational background, half of participants had Bachelor degrees, 7 were school leavers, and 3 had Master degrees. Participants had a broad range of occupations: 8 in administrative roles, 4 in financial and marketing sector, 3 school teachers, 2 unemployed, 1 in medical field, 1 in IT and 1 student. Each participant was rewarded RM50 (equivalent to £10 in Malaysian currency). Participants were recruited from five Facebook and Telegram groups of Malaysian bitcoin users, joined by the second author. Malaysia offers a specific opportunity for the exploration of bitcoin practices. On the one hand, despite five decades of economic growth, it is still a developing country with increasing inflation rate, underdeveloped democracy and a financial system which is now under the scrutiny of law enforcement. On the other hand, Malaysia experiences a massive growth of remittance and payment market, and interest in crypto currency, being in 2016 the first developing country considering Fintech regulation. Over the last year it also ranked fourth on bitcoin searches on Google Trends, and first among developing countries on the number of bitcoin nodes.

The invitations for taking part in the study were both publicly posted and privately sent to the most active members in each of the online groups. We also applied snowball sampling so that six more participants were introduced by the interviewed ones. We conducted semi-structured interviews between April and May 2016, to explore users' motivation, understanding and use of bitcoin. We asked: "*why are you interested in bitcoin*", "*how did you learn about bitcoin*" and "*which are the benefits and challenges of using bitcoins*". We also asked about users' challenges and trust-related issues: "*what are the challenges that you face when using or engaging with*

bitcoin technology", and "*how much trust do you have in bitcoin technology*", and followed up with additional questions on perceived security and anonymity. Not at least, we explored participants' perception of risk and their mitigation strategies: "*did you experience any fraud*", and "*will you take any actions to prevent that in the future*".

The interviews took place via Skype or phone. They lasted at least an hour, were audio recorded and fully transcribed. The analysis involved a hybrid approach where existing concepts were used for the deductive coding while new concepts grounded on the empirical data, contributed to the inductive coding [19]. The deductive coding included concepts from the HCI literature on trust such as technological, social and institutional dimensions of trust [43], factors of user's trust in technology such as credibility, ease of use, and risk [13], and properties warranting trust between technology users such as temporal, social and institutional embeddedness, as well as credibility, integrity and benevolence [41]. We have also used concepts related to blockchains' characteristics such as decentralization, unregulation, pseudo-anonymity, as well as transparent and irreversible transactions. The coding list was iteratively refined in the light of the interview data, as new codes emerged under the theme of motivation, insecure transactions and risk mitigating strategies.

RESULTS

We start by outlining users' motivation for engaging with bitcoin technology, followed by a description of its key characteristics and their impact on users' trust. In particular, we highlight the issue of insecure transactions and the associated human and technology-related risks. We further unpack the risks of dealing with dishonest traders, and the mitigating strategies for addressing them.

Motivation for the Use of Bitcoin Currency

This section highlights the motivation of end users, people with limited knowledge of bitcoin technology, who adopt and engage in the use of bitcoins. The motivation and perception of early adopters towards bitcoins can be grouped according to Davis' technology acceptance model [16] in perceived usefulness, and ease of use. We further describe the perceived usefulness of bitcoins as an external motivational factor and its key economic rationale.

Economic Rationale

The economic aspect captures people's distrust in financial institutions and the governments legitimizing them. Several participants referred to the importance of protecting one's savings in the face of an unstable economic climate, dominated not only by inflation but also by governments' decisions to control personal bank account holders' money and their movement [11]. For example, the following quote is illustrative for a quarter of our participants: *"From what I learned from the Cyprus crisis, governments and banks have the authority to take your money from your account […] the trust in financial institution is gone forever. So I looked for alternatives and found Bitcoin to keep the savings"* [P16]. This outcome provides support for the security motive for acquiring money and bitcoins' perceived value for providing safety when people distrust the world and the future [22], particularly in the context of inflation and economic downturn: *"currently our currency is falling and I am worried. As a backup plan, I converted my money in gold or bitcoins, which are not influenced by any big parties or power"* [P8]. This is interesting as reflects the assumption of gold as commodity, which wrongly conflates gold's long-run price stability with the absence of power for regulating its price: while such power does not need to belong to centralized banks, it still requires government's authority [6].

A third economic reason underpinning the adoption of bitcoins is speculation on their future value. Almost half of participants share this view: *"I keep my saving in bitcoins [because] their future value will increase over time"* [P11]. In such cases, participants purposely explored alternative means of exchange for replacing their volatile fiat currency in order to both protect savings and more importantly, to invest for future income.

Social Learning

Findings indicate that in order to learn about the bitcoin currency, participants leverage the emerging social network of bitcoin users. This social aspect underpinning the initial motivation of bitcoin's early adopters include online communities where most of participants have heard for the first time what bitcoin currency is: *"The first time I heard [about bitcoins] was from the Reddit forum"*. After finding out about the bitcoin currency and its potential value, participants described their efforts to learn more through self-guided online research: *"First I read about bitcoin online in 2009, [and] in 2013 I could see the price rising up, so I started to learn more about"* [P7]. An additional source of information about bitcoin is peers and friends: *"I started to know about bitcoin a few years ago, when my friend told me about the wallet, the process and how bitcoins could eliminate banks' transactions"* [P3].This quote indicates how some early adopters champion the use of bitcoin currency by highlighting its advantages against the national fiat currencies.

Uses of Bitcoins

While most of the literature describes bitcoins as cryptocurrency [8,12], our findings indicate that they are used predominantly as store of value, i.e., predictably valuable for later use. Eight participants used bitcoins on a regular basis to generate income, 7 used them occasionally for investment, while 5 were full time investors. This is interesting, because, bitcoins experience high volatility which makes them on the long-term unreliable stores of value [52]. It appears that the complete control over one's savings is preferred over the less volatile yet less controllable fiat currency. Such characteristics were shared by other cryptocurrencies such as litecoin and swisscoin also used by our participants.

Another surprising finding is that we have seen only three isolated accounts of the use of bitcoin as currency for buying goods or services, despite the growing number of merchants who accept bitcoins (Figure 1). Most of the payments were for online utility or phone bills, food, or mining equipment. For example one participant noted the payment of his mobile phone's prepaid credit with bitcoins [P10], while another referred to the payment of food supplement from a friend: "*he just sent me his QR code and I scanned the code and transferred the amount of bitcoins* " [P19]. In addition one participant mentioned both online and offline uses of bitcoin currency: "*I pay my utility bills in bitcoins from the cryptomarket.my. I even buy my cigarette from expedia.com, and use cheapair.com to buy my flight tickets and hotel bookings too. Then there is a restaurant in Johor where I pay in bitcoins*" [P12]. This diverse way of spending bitcoins as currency is an exception rather than the norm, as we failed to find any additional participants reporting similarly rich use of bitcoin currency. Interestingly, we only found one account of illegal purchase: "*I bought an unlimited Spotify account from the dark web using bitcoin*" [P1].

Blockchain's Characteristics and their Impact on Trust

We now describe the main characteristics of bitcoin technology, and how they contribute to trust in bitcoin. These include blockchain's decentralization, unregulation, embedded expertise and reputation, as well as transparent, low cost, easy, and insecure transactions.

Decentralized Blockchain

One of the main identified characteristics relates to the decentralized nature of bitcoin technology [47]. Findings indicate that most participants appreciate that bitcoin transactions do not involve any third party involvement from financial institutions: *"A decentralized currency is a bit more secure in terms of handling it is same like an asset. So if nobody else [third party] handles the asset, it is more secure for me to handle it by myself"* [P20]. The decentralization of blockchain also fosters confidence in its clear intention to circumvent, arguably dishonest central financial institutions. This in turn provides support for honesty as a dimension of credibility in Corritore and colleagues' [13] model of online trust.

People also understand the reduced need for the complicated authorization process for sending and receiving money: *"if you look at the current banking system, it takes three working days to do the settlement, but with blockchain you can settle it instantly"* [P3]. This quote illustrates the appreciation for quicker transfer of money between accounts, and therefore the ease of use.

Unregulated Blockchain

Participants also expressed appreciation for the unregulated aspect of blockchain technology. As a result, more than half of participants perceive this as an opportunity to become more empowered and privileged to regain control over their own money: "*All governments love to control people [but] they cannot control bitcoin, and that's why they cannot accept it. Bitcoin is people's money giving them financial freedom*" [P14]. This is a militant statement, which links back to the initial motivation for engaging with blockchain technology: the erosion of trust in financial and government institutions coupled with the economic crisis [43].

Unregulation sets no limits for sending and receiving money, which can take place either locally or worldwide: *"I see no boundaries for people to do trading globally or nationwide; a freedom to do the trading without any restriction from the authority"* [P2]. As a decentralized and unregulated system, the risk of abuse of power over individuals' personal assets is highly restricted. This confirms a limitation of the perceived risk as the third dimension of the model of online trust [13]. Several participants referred to the benefits of blockchain's pseudo-anonymity, and its value in supporting unregulation as illustrated by this quote: "*we can keep our money as much as we want and the government will not able to freeze our wallet because of the pseudo-anonymity*" [P11].

Blockchain's Embedded Expertise

Another characteristic of bitcoin technology is people's appreciation for the expertise required for mining bitcoins and verifying transactions. This is interesting giving that for example, mining a rig needs limited technical knowledge. Findings however indicate that the cost required by the mining process provides a guarantee for the invested expertise and ultimately for the credibility of the blockchain technology: *"producing bitcoins is not something easy. There are specific ways to mine and expensive equipment needed"* [P8]. As the competition and difficulty for mining bitcoins increases over time, more computationally intense mining equipment is needed which in turn lead to higher costs for producing bitcoins. Almost a quarter of participants mentioned this complexity and the cost of the mining procedure. Their appreciation for miners' expertise fosters credibility in bitcoin currency and transactions. This further confirms the credibility dimension of the online model of trust and its application to bitcoin technology [13].

Blockchain's Reputation

The reputation of the blockchain technology has been notoriously damaged due to illicit activities on Silk Road, an anonymous online marketplace predominantly for narcotics, which uses bitcoins as its exchange currency [10]. Four participants mentioned such reputation issue due also to current cybercrimes, since Silk Road was closed down in 2013: "*there are lot of crimes due to bitcoin's anonymity: money laundering, terrorist financing and tax evasion*" [P15] but surprisingly, with limited reference to its negative impact on participants' credibility in bitcoin technology. Interestingly, we also found instances where participants in fact valued the growing reputation of bitcoin technology: *"In the long term, this technology has a very bright future. There are lots of big companies which start doing research on blockchain"* [P17]. This quote suggests

that the large companies' interest in blockchain offers alternative routes for legitimizing its authenticity and ultimately credibility. Apart from trust in blockchain, participants also referred to trust in bitcoin transactions. We now discuss the main characteristics of bitcoin transactions and how they support or hinder trust.

Transparent Transactions

Our findings indicate an important and valued characteristic of bitcoin transactions: their transparency [47]. The public ledger allows public access to the movement of bitcoins from one wallet to another. Users are able to track any bitcoin transactions from the very first one, until the present day: *"because bitcoin uses blockchain, we can see the movement of the bitcoins in a public ledger. It is very transparent"* [P11]. Transparency echoes technology's credibility dimension in Corritore and colleagues' [13] model of online trust, and its honesty dimension.

Easy and Quick Transactions

Another valued characteristic of bitcoin transactions is their ease and speed of completion: "*With bitcoin you can move your money globally in just a second; very easy*" [P11]. A similar quote emphasizing the ease of completing worldwide transactions by comparing them with the ease of texting: "*It is easy to move money from one country to another. It is just like you send a text message and the transaction is done*" [P13]. The above outcomes suggest that through transparent, easy, and quick transactions, people experience ease of use. According to Corritore and colleagues' [13] model of online trust, ease of use is one of the three factors of trust.

Low Cost Transactions

A third valued characteristic of bitcoin transactions is their low cost. A few participants provided quotes to support this: "*it only costs me 10 cent for each transaction*" [P6]; or "*the main benefit of transactions is that they are easy, fast and cheap*" [P14]. These outcomes indicate that transactions' low cost could further contribute to reducing transactions' perceived risk, as participants do not have to fear hidden or higher costs. In their model of online trust, Corritore and colleagues' [13] referred to risk as the third factor of trust, and explained the direct relationship between users' perception of control and their trust. If the above characteristics support users' trust in their bitcoin transactions, findings also indicate one characteristic which hinders trust which is further detailed.

Insecure Transactions

An important finding is that despite the above characteristics supporting trust in blockchain technology and bitcoin transactions, participants also reported their concerns about the risk associated with insecure transactions. It is worth mentioning that insecure transactions do not concern miners' cryptographic protocol for authorizing transactions. Indeed, none of participants reported concerns about the security of this protocol, but strong trust in miners' expertise and in the predictability of the protocol. Instead, insecure transactions relate to human error or malice and technology's limitation to address them. More specifically, we identified four types of insecure transactions, three related to human factors: those due to users themselves, to the other person or entity engaged in transaction, or to the third human parties not engaged in transactions; and one related to technology's limitation to address them. We now discuss the associated risks for each of these types of transactions.

Risks Due to Users' Challenges of Handling Passwords

Six participants mentioned the risk of losing the password for their wallets, or the risk of insufficiently protecting it. For example, the quote below illustrates this type of risk and its serious consequence of no longer being able to access one's bitcoins from that wallet: "*Make sure you don't forget your password because blockchain does not keep your password […] it cannot be recovered and you will lose all your bitcoins from that wallet*" [P16].

The second risk of insufficiently protecting the password can have equally serious consequence of having the bitcoins stolen: "*I lost 30 bitcoins in the last months because of my own security mistake. I set up my wallet password the same as my email password. One day, my wife clicked on a phishing email and the hackers were able to get my email password and use it to log in to my bitcoin wallet*" [P12].

In order to address these risks, some users mentioned the importance of taking responsibility for securely storing and protecting their passwords: *"As users we must know how to make sure that our bitcoins are secured. It is the same as protecting our own cash or any personal valuable thing that can be stolen by others"* [P15]. Some participants even installed additional security applications in their bitcoin wallet such as double authentication [P12], since although "*the system is secured, the security responsibility is with the user. If anyone lost their bitcoins, the first person to be blame is themselves, not the system*" [P14].

Risks Due to Hackers' Malicious Attacks

Three participants mentioned that insecure transactions are also due to malicious hacker attacks. We have seen above that some of these involve phishing emails to target wallet passwords. Such attacks can penetrate even through double authentication: "*you must make sure that your password is difficult to guess. A friend lost 14 bitcoins even though he applied double authentication on multiple devices*" [P11].

Risks Due to Failure to Recover from Human Error or Malice

Although a third of participants considered themselves responsible to secure their bitcoins, a few also indicated that the recovery from users' failure to protect their passwords or from hackers' attacks is limitedly supported by the bitcoin technology. The main imitation here is that transactions are irreversible: "*let's say the hacker has diverted the money to another bitcoin wallet address; you will never know where your money has been transferred to and you cannot reverse the transaction either*" [P1]. This is

an interesting finding, indicating a drawback of the blockchain technology. The rationale for irreversible transactions addresses the limitation of the centralized financial system which allows reversible transactions without being bound to enforce the parties' contract stating that the sale is final [39]. However, as suggested in the above quote, this design feature fails to account for malicious transactions due to hacking, or to the dishonesty of the trading parties, as further detailed.

It is important to make the distinction between how transactions are represented in blockchain, i.e., data structure allowing the transfer of bitcoins from one electronic wallet to another; and how our participants perceive transactions: a two-way transfer of bitcoins and money/goods. Unlike the one-way remittance transactions well supported by the bitcoin technology [27], all transactions reported by participants are two-way, with both parties sending and receiving assets. Although most transactions involve buying or selling bitcoins against fiat currency, participants were only able to track one side of the transaction, namely the movement of bitcoins captured within the blockchain. This raises major risks and trust issues particularly in relation to potentially dishonest trading partners, as the untracked part of transaction does not allow for scrutiny. This issue is further emphasized when dealing with traders who are not authorized entities.

Risks Related to Dishonest Partner of Transaction

Findings indicate that a considerable risk factor is dishonest partners with whom one engages in bitcoin transactions. A quarter of participants reported incidents where either them, or their close friends have been cheated and their trust betrayed: "*I transferred some bitcoins but the buyer didn't pay me*" [P6]. This quote illustrates the importance of knowing about the transaction partner. This point has been mentioned by other participants who expressed concerns about strangers' unknown reputation: *"you don't know whether the seller is scam or not*" [P1].

Strategies for Mitigating the Risks of Dishonest Traders

We identified five strategies for dealing with dishonest transaction partners, and for mitigating their risks. These strategies involve two forms of trading: directly with another person, or through online exchanges, i.e. services for matching price and offer between bitcoin sellers and buyers. These strategies are further described starting with the most frequent one, and we shall see that the running themes across these strategies are the traders' pseudo-anonymity and the unregulation of blockchain technology.

Trade with Authorized Exchanges

The online exchange is by far the first and most preferred form of transaction, mostly because its regulation supports users' trust. Indeed, although bitcoin technology and its cryptographic protocol are unregulated, exchanges require authorization from the financial services such as Financial Conduct Authority [54]. For example, five participants mentioned their check of exchangers' credentials: *"I do look at their background, and legal term conditions and from there I put trust on the exchange"* [P2]. The exchanges' websites are crucial for fostering trust: *"a proper website, [indicating the amount of] trading, and testimonials [supports] trust on the exchange"* [P3].

This extends previous HCI findings on the value of website for trust [3,38], to the context of cryptocurrency transactions. An additional source of trust is the option to contact directly the exchange's agents: *"I prefer this exchange because they have their representative to contact if there is any problem or question to ask"* [P12]. In turn, this makes users' relationship with the exchanges, a more personal one. Apart from being authorized by financial services, and having credible websites, exchanges also foster trust in transaction partners, as they require sellers and buyers to register and have their identity verified. This is an important finding, indicating ways to address the extensive concerns around traders' pseudo-anonymity. Surprisingly, only one participant reported the use of the escrow service (third party holding the assets to be released once both parties are satisfied with the transaction). Findings indicate that ease of use is negatively impacted by the use of the escrow, because of its additional registration requirements: "*it is easier and faster to do the transaction [directly] with other traders*" [P10].

These findings provide support for the contextual properties described in the framework on mechanics of trust [41], warranting users' trust in exchanges because of their successful performance and the expectation that they will perform consistently well in the future (temporal embeddedness), exchanges' reputation (social embeddedness), and their legally authorized services (institutional embeddedness). We also found evidence for the intrinsic properties warranting trust in exchanges, for example through social presence of professional websites and contactable local representatives (integrity), as well as reputation through testimonials (credibility).

Trade with Socially Authorized Traders

In comparison with exchanges, dealing with individual traders offers weaker risk mitigating strategies. The strongest strategy is dealing with socially authorized traders. These are well-known, de-anonymized members of online groups who regularly join discussions and trade bitcoins. Thus they become trusted and their names are added by the group administrator to an online list of verified traders: "*I only buy from authorized traders as lots of friends experienced scam and huge losses*" [P18]. The label of authorized trader is usually provided within an online group of bitcoin users on the basis of a series of successful de-anonymized transactions. This outcome indicates the crucial value of de-anonymity for credibility and trust. These findings also provide evidence for the framework on mechanics of trust [41] warranting users' trust in authorized traders (temporal and social embeddedness), but limited institutional embeddedness.

Trade with Reputable Individual Traders

If an authorized trader cannot be found, participants engage in a weaker risk mitigating strategy: dealing with reputable traders. Unlike traders authorized by an online user group, reputable ones benefit only by credibility by proxy, from a few group members who have engaged in successful transactions with these traders. For example, participants indicated the use of peers' or friends' recommendations: *"I knew the trader from the telegram group, and a few recommendations from friends who can be trusted"* [P8]. Almost half of participants noted that their first point of contact for background check on an unknown trader is their online groups *"If I am dealing with stranger, I will ask in my online group to verify that particular person. If they don't know him I will not proceed with the transaction"* [P10]. In addition, more than half of participants mentioned their preference for known traders whom they have had successfully trusted in the past: *"Most of them are my close friends, so I have no problem trusting them"* [P20]. This shows the value of reputation and benevolence in supporting traders' credibility [13]. These findings confirm the framework on mechanics of trust [41] warranting users' trust in traders because of their reputation (social embeddedness and credibility), and when dealing with friends, because of perceived integrity and benevolence.

Trade with De-anonymized Individual Traders

Although less common and mostly due to lack of experience, sometimes bitcoin users engage in transactions with unknown traders. In such cases, findings indicate that seldom the traders remain unknown, as we identified two mechanisms for ensuring traders' de-anonymization: face to face meeting, or online sharing of their IDs. For example, several participants expressed the view that they only proceed with the transaction if the trader is willing to de-anonymize. One way of achieving this is through face to face meeting, where both sides of the transaction take place simultaneously, i.e., the exchange of bitcoins and fiat currency or goods: *"We cannot trust them online. We need to see that person and to do cash on delivery"* [P4]. Other participants require traders to de-anonymize by emailing their copy of personal ID: *"I need to know their identity"* [P5]. This strategy does not provide any contextual factors to allow users' trust in unknown traders for whom they have no reputation-related information (neither social nor institutional embeddedness) [41]. Hence, users attempt to develop institutional embeddedness by de-anonymizing the traders, or by reducing the risk of asynchronous transaction altogether through face to face meetings to perform synchronous two-way exchanges.

Regulating Bitcoin

In order to address the challenge of dishonest traders, many participants expressed the wish that bitcoin becomes regulated: "*I think we must demand to our politicians to regulate bitcoin*" [P1]. This is an important finding indicating a higher level strategy which does not address the trading itself but the unregulated nature of blockchain.

THEORETICAL IMPLICATIONS

We now reflect on the value of these findings for advancing the HCI discourse on trust. We also discuss the specific tensions that unregulation and pseudo-anonymity bring to trust. Our implications are mostly relevant for bitcoin users in developing contexts. They may also hold value for understanding and supporting trust in cryptocurrencies in general in both developing and developed contexts, but future work is required to explore this.

Towards a Model of Trust among Bitcoin Users

Our findings advance the understanding of users' trust in blockchain technology and in transaction partners. We argue for the feasibility of the considered HCI theories [13,41,43] for identifying key blockchain's characteristics supporting users' trust: decentralization, unregulation, miners' expertise, as well as transparent, easy, and low cost transactions. The main trust challenge experienced by bitcoin users is the risk of insecure transactions, and in particular that of dealing with dishonest traders.

We start by discussing the findings in the light of Sas and Khairuddin's [43] bitcoin trust framework. Our findings suggest that technological trust of bitcoin users in blockchain technology is strong, as participants value its secure cryptographic protocol. This extends prior findings on users' challenges to secure their bitcoins [29] with their willingness to take responsibility for their weak, easy to break wallet passwords.

Findings also indicate novel insights into the social dimension of trust among bitcoin users. The main challenge here relates to dishonest bitcoin traders. With respect to different stakeholders, it is worth mentioned that our findings capture the blurring of the boundaries between merchants and users when the object of transaction is bitcoins. In fact, we found little evidence that bitcoin users engage with merchants to buy goods, indicating participants' preferential use of bitcoin as a store of value rather than currency. Our outcomes also suggest extending this framework's definition of institutional trust to include not only government trust in blockchain technology but also the trust of bitcoin users in government and financial institution. We have also seen evidence for how the erosion of such institutional trust is crucial in users' adoption of bitcoin and acceptance of its *algorithmic authority* [33].

Probing further into the exploration of technological trust, we applied the model of online trust [13] to identify specific blockchain's characteristic impacting on trust. Our findings provide support for extending the applicability of this model to bitcoin technology. Blockchain's characteristic supporting users' credibility include: honesty ensured by decentralization and public ledger's transparency; expertise supported by miners' competence and hard labor; predictability supported by the cryptographic protocol; and reputation supported by large companies' interest in bitcoin. Findings also identified blockchain's characteristics supporting the other dimensions of trust: ease of use

grounded in ease and quick transactions; and limited risk due to transactions' low cost and the decentralized, unregulated nature of blockchain which limits the risk of institutional power abuse. Outcomes also suggest a specific technological characteristic perceived as a risk factor: the blockchain's purposeful design feature for irreversible transactions. We found the challenge of two-way transactions and in particular the offline one which is not captured by the blockchain. The challenge of irreversible transactions is not grounded in people's distrust on transaction, but in potentially the dishonest part of transaction, i.e., the payment of fiat currency for acquiring the bitcoins. If this side of agreement is not fulfilled, users would prefer to reverse the bitcoin transaction, an operation which is not possible. An interesting design opportunity here would be exploring new ways of tracking this movement of fiat currency (currently not captured) in the blockchain.

As a means of exploring users' support for trusting their transactions partners, we applied the framework on mechanics of trust [41]. This framework allowed the identification of different sources of trust for each of the risk mitigating strategies. Among these strategies for dealing with dishonest traders, bitcoin users engage in decreasing order of preference with exchanges, authorized or reputable traders, and ultimately with unknown traders which they attempt to de-anonymize. Only the exchangers provide legally authorized services [37,52], while trust in the other types of traders is supported mostly by the information about their credibility and reputation within the thick relationships [24] of online user groups. The less reputation-related information users can gather about the traders, the stronger the need to de-anonymize them. Most participants went even further suggesting the value of regulating the blockchain (institutional embeddedness for all types of traders).

The Paradox of Unregulation

We argue that the exploration of bitcoin use offers an unprecedented opportunity for questioning common assumptions that people hold about fiat money and in particular around the value of money, their control and legitimacy. Blockchain's unregulation and the pseudo-anonymity of people behind transactions are crucial characteristics of this technology [18,28,46,49]. Together, these characteristics ensure the privacy of the owners of bitcoin addresses, which is central to Nakamoto's vision [39]. Our findings however highlight an interesting tension: bitcoin users desire regulation, mostly because of the challenge of dealing with dishonest traders, which they believe may be addressed by de-anonymizing transaction's parties. This is an important finding as the efforts to regulate bitcoin have been driven mostly by government and financial institutions rather than users [21]. Users' desire for regulation may be also related to the new forms of thinking that a disruptive technology like bitcoin demands. Bitcoin provides freedom over one's assets which many participants enjoy, but at the same time, it no longer provides the security that regulated financial institutions provide, and which users are accustomed with. We argue that at present, bitcoin users continue to operate under the old mind-set of fiat money in traditional centralized and regulated financial systems, and may need support for developing new mental models underpinning the unregulated bitcoin technology. This calls for new ways of supporting users to further develop their digital literacy. It also calls for the exploration of innovative technological and social mechanisms for limiting the impact of dishonest traders, while still preserving anonymity.

The Challenge of Pseudo-anonymous Transactions

Our findings indicate that blockchain's deliberate pseudo-anonymity of users engaged in bitcoin transactions becomes a challenge for the contextual properties for warranting trust as described in the framework on mechanics of trust [41]. This is because all three forms of temporal, social and institutional embeddedness would become effective only through the known and stable identities of bitcoin users across transactions. This would ensure that the transaction partners build together a history of transactions (temporal), and a reputation among other potential transaction partners (social), while becoming vulnerable to legal sanctions when they dishonestly fail to meet their transaction agreement (institutional embeddedness). However, neither of these is possible, as the blockchain protects the privacy of the transaction parties, both by preventing the link between the wallet address and the owner's identify, and by enabling the loss of the link between user's transactions over time, i.e., through the option of creating new wallet addresses for each transaction [39]. This is problematic, as blockchain's failure to support for contextual properties motivating users to fulfil their agreements [41], means that such fulfilment relies entirely on the trustees' intrinsic properties such as credibility, integrity, and benevolence or encapsulated interest [24]. We found however significant evidence that people do not trust the intrinsic properties of the trustee, and aim to protect themselves by challenging the trustees' pseudo-anonymity as one of blockchain's key designed feature [39]. This confirms findings on people's readiness to take very small risks regarding unknown trustees [24].

DESIGN IMPLICATIONS

Now we turn our attention to the design implications [44] that our findings suggest. We discuss the need to support the transparency of two-way transactions, tools for materializing trust, and tools for supporting reversible transactions. These design implications have been developed to address the identified trust challenges of dishonest traders, while respecting blockchain's main characteristics such as decentralization, unregulation and pseudo-anonymity.

Supporting Transparency of Two-way Transactions

All transactions reported in the study are two-way, most of them sequential and asynchronous, i.e., typically one party sends the fiat currency and after receiving it, the other party

sends the bitcoins. However, people can only track on the blockchain the movement of bitcoins. Sending fiat currency can be faked through fraudulent statements of transfer. This coupled with the lack of legally authorized partners warranting one's trust in them, i.e., institutional embeddedness, leads to increased risk of defraud from dishonest traders. Such traders are not known and cannot be made accountable for failing to complete their part of transaction, neither responsible for the retribution it entails.

One can imagine creative design methods [42] and new tools for digitally capturing the contents of transactions which is not bitcoins, to ensure that their transfer is also verified, authorized and stored on the public ledger. Our findings indicate that such content of transaction is often fiat currency. Blockchain already provides mechanisms for creating digital tokens backed by fiat currency, i.e., Colored Coin, Omni Layer [48]. Such mechanisms can also be harnessed for creating digital tokens (metadata embedded in the blockchain) backed by physical goods, such as the ones explored in the provenance context where tokens represent documents accompanying the transaction of goods or finances as means of tracking their ownership. Such mechanisms need to remain decentralized and to become integrated into the blockchain interface so that end users with limited technical expertise can access and use them.

Tools for Materializing Trust in Blockchain

Findings indicate that in the absence of known and stable identities, bitcoin users who engage in transactions with each other rely mostly on social embeddedness. As one of the properties warranting trust in another party [41], social embeddedness is reflected in users' active effort to gather reputation-related information about unknown traders, either from people they already trust such as close friends, or from members of the online group where most of their social learning about bitcoin technology takes place. One way to better support this data gathering is through designing mechanisms for capturing and visualizing reputation as meta-data linked to a wallet address. Blockchain protocol already supports the creation of metadata within a transaction, by allowing the generation of a new secure address referencing the metadata. A reputation management system built on top of the blockchain will strongly contribute to the social embeddedness for warranting trust among traders. This in turn, motivates traders to keep the same wallet address in order to grow their reputation, hence providing more stable, albeit still private, identities. For example, Carboni [7] proposed vouchers attached to transaction for the transfer of payment for a service. If the buyer is satisfied with the service, he can accept and co-sign the voucher which contains an incentive fee paid by the service provider to the buyer for leaving a positive feedback. The reputation score of a service provider could be computed by adding the voting fees for that service across blockchain's relevant transactions. Alternative mechanisms for supporting also the caption of negative feedback are much needed.

Tools to Support Reversible Transactions

Findings indicate that in the case of dishonest traders, the irreversible bitcoin transactions are problematic. This stems from the lack of transparency of the two-way transactions: while the transfer of bitcoins is captured by the blockchain, the counterpart asynchronous transfer of money (or goods) for which people receive (or pay bitcoins) is not. One way of addressing this is by exploring novel mechanisms for reversing individual two-way transactions on top of the irreversible blockchain protocol [2]. This is not a trivial issue, as in its current form, the blockchain protocol does not allow reversing transactions which have been already confirmed and added to the ledger. One solution would be new tools for enabling the de-anonymization of the owner of disposable wallet addresses (discarded after one use). Besides hindering dishonesty, such tools would allow users' to protection their privacy on the blockchain, while enabling them to contact the other party, and request reversing the bitcoin transfer. This would also support social embeddedness, as the reputation of a given trader operating in a local online group can well extend beyond the lifetime of a disposable wallet. Other tools could leverage the support of multisignature transactions enabled by the bitcoin protocol [2]. A common example is 2-of-3 transaction model where money is placed in a joint address owned by the both parties and a third arbitrator, to be signed off once each party is satisfied. If there is a problem, the arbitrator will investigate and decide to transfer the payment back to the buyer or to the seller. Once the transaction receives 2 out of 3 signatures, it is completed. The multisignature tools differ from the escrow services as the arbitrator receives a fee agreed by all three parties, but cannot defraud as he will need two signatures for this. Surprisingly, no participant mentioned the use of multisignature tools, probably because of the same reason they do not engage with the escrow services: perceived difficulty of use, or limited awareness of such tools. Future work could further explore this.

CONCLUSIONS

This empirical study investigated blockchain's characteristics which support and challenge users' trust, alongside their motivation for bitcoin use, and strategies for mitigating identified risks. We advance the theory towards a model of trust among users of Bitcoin's decentralized, unregulated and pseudo-anonymous technology in developing context, and provide insights into the specific tensions around these characteristics. Study findings led to a number of design implications that would support bitcoin users develop increased trust in each other, including support for the transparency of two-way transactions, tools for materializing trust, and tools for supporting reversible transactions.

ACKNOWLEDGEMENTS

This work was supported by the UK Research Council through the Digital Threads project, (AHRC Grant AH/P014186/1).

REFERENCES

1. Michael Bacharach and Diego Gambetta. 2003. Trust in Signs. In *Trust in Society,* Karen S. Cook (ed.),. Russell Sage, New York.
2. Rachid El Bansarkhaniand Jan Sturm. 2016. An Efficient Lattice-Based Multisignature Scheme with Applications to Bitcoins. In *International Conference on Cryptology and Network Security*, 140-155.
3. Ardion Beldad, Menno de Jong and Michaël Steehouder. 2010. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in human behavior* 26, 5: 857-869.
4. Bitcoin Wiki. Anonymity. Retrieved September 14, 2016 from https://en.bitcoin.it/wiki/Anonymity
5. Mads Bodker. 2004. Trust and the digital environment. Retrieved June 10, 2016 from http://www.itu.dk/people/boedker/trustpaper.pdf
6. Michael Bordo. 1981. The classical gold standard: some lessons for today. *Review*, 2-17.
7. Davide Carboni. 2015. Feedback based Reputation on top of the Bitcoin Blockchain. Retrieved September 19, 2016 from arXiv preprint arXiv:1502.01504
8. Raul Carillo. 2015. Alternative currencies are bigger than bitcoin: how they're building prosperity from London to Kenya. Retrieved June 22, 2016 from http://www.yesmagazine.org/commonomics/alternative-currencies-bigger-than-bitcoin-bangla-pesa-brixton
9. John M. Carroll and Victoria Bellotti. 2015. Creating Value Together: The Emerging Design Space of Peer-to-Peer Currency and Exchange. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*, 1500-1510.
10. Nicolas Christin. 2013. Traveling the Silk road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web*. ACM, 213-224.
11. CNN Money. 2015. Greece shuts banks in bid to prevent collapse. Retrieved June 10, 2016 from http://money.cnn.com/2015/06/28/news/economy/greece-banks-ecb/
12. Coin Market Cap. 2016. Crypto-currency market capitalizations. Retrieved June 10, 2016 from https://coinmarketcap.com/
13. Cynthia L. Corritore, Beverly Kracher and Susan Wiedenbeck. 2003. *International Journal of Human-Computer Studies* 58, 6: 738-758.
14. Robert Costanza, et. al. 2003. Complementary currencies as a method to improve local sustainable economic welfare. Retrieved June 10, 2016 from http://78.46.126.155/Record/632
15. Michael Crosby, Nachiappan , Pradhan Pattanayak, Sanjeev Verma and Vignesh Kalyanaraman. 2015. Retrieved June 10, 2016 from http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf
16. Fred D. Davis. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* 13, 3: 319-340.
17. Encyclopedia.com. 2002. Coins and currency. Retrieved September 19, 2016 from http://www.encyclopedia.com/topic/coin.aspx European Central Bank. 2012. Virtual currency schemes. Retrieved June 10, 2016 from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf
19. Jennifer Fereday and Eimear Muir-Cochrane. 2006. Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International journal of qualitative methods*, *5*, 1: 80-92.
20. Amy Fontinelle. 2011. An introduction to complementary currencies. Retrieved June 10, 2016 from http://www.investopedia.com/articles/economics/11/introduction-complementary-currencies.asp
21. David Gilbert. 2016. Bitcoin's big problem: transaction delays renew blockchain debate. Retrieved June 10, 2016 from http://www.ibtimes.com/bitcoins-big-problem-transaction-delays-renew-blockchain-debate-2330143
22. Herb Goldberg and Lewis Robert. 2000. Money madness: The psychology of saving, spending, loving, and hating money. Wellness Institute, Inc, Gretna LA,
23. Andres Guadamuz, Chris Marsden Guadamuz. 2015. Blockchains and Bitcoin: Regulatory responses to cryptocurrencies. *First Monday*, 20: 12-7.
24. Russell Hardin. 2002. Trust and trustworthiness. Sage Foundation, New York.
25. Garrick Hileman. 2014. From bitcoin to the brixton pound: history and prospects for alternative currencies. In *International Conference on Financial Cryptography and Data Security* ,163-165.
26. Jofish Kaye, Janet Vertesi, Jennifer Ferreira, Barry Brown, and Mark Perry. 2014. #CHImoney: financial interactions, digital cash, capital exchange and mobile money. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems* (CHI EA '14). 111-114.
27. Erol Kazan, Chee-Wee Tan, and Eric TK Lim. 2015. Value Creation in Cryptocurrency Networks: Towards A Taxonomy of Digital Business Models for Bitcoin Companies. *The 19th Pacific Asia Conference on Information Systems (PACIS 2015)*.
28. Irni Eliana Khairuddin, Corina Sas, Sarah Clinch, and Nigel Davies. 2016. Exploring Motivations for Bitcoin Technology Usage. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems*. ACM, 2872-2878.
29. Brad Klontz, Sonya L. Britt, Jennifer Mentzer, and Ted Klontz. 2011. Money beliefs and financial behaviors: Development of the Klontz Money Script Inventory. *Journal of Financial Therapy* 2,1.

30. Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer and Edgar Weippl. 2016. The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. *Financial Cryptography and Data Security*.
31. Sara Lipkis and Amanda Roth. 2016. Anatomy: what is alternative currency? Retrieved June 10 2016 from http://www.worldpolicy.org/anatomy-what-alternative-currency
32. Niklas Luhman. 1979. Trust: a mechanism for reduction of social complexity. In *Trust and Power*, Niklas Luhmann (ed). Wiley, New York,
33. Caitlin Lustig and Bonnie Nardi. 2015. Algorithmic authority: The case of Bitcoin. In *System Sciences (HICSS), 2015 48th Hawaii International Conference IEEE.* 743-752.
34. Roger C. Mayer, James H. Davis and F. David Schoorman. 1995. An integrative model of organizational trust. *The Academy of Management Review* 20, 3: 709
35. Barbara A. Misztal. 1996. *Trust in Modern Societies. The Search for Basis of Social Order*. Cambridge University Press, Cambridge, 42-87.
36. Guido Mollering. 2006. *Trust: Reason, Routine, Reflectivity*. Elseiver, Netherlands.
37. Malte Moser. 2013. Anonymity of bitcoin transactions: an analysis if mixing service. RetrievedJune 10, 2016 from https://www.wi.unimuenster.de/sites/wi/files/public/department/itsecurity/mbc13/mbc13-moeser-paper.pdf
38. Fiona F. Nah and Sid Davis. 2002. HCI research issues in e-commerce. *Journal of Electronic Commerce Research* 3.3: 98-113.
39. Satoshi Nakamoto. 2008. Bitcoin: peer to peer electronic cash system. Retrieved September 14, 2016 from https://bitcoin.org/bitcoin.pdf
40. P2P Foundations. 2015. Definition of Bitcoin. Retrieved June 10, 2016 from http://p2pfoundation.net/bitcoin
41. Jens Riegelsberger, M. Angela Sasse and John D. McCarthy. 2005. The mechanics of trust: a framework for research and design. *International of Human-Computer Studies.* 62, 3: 381-422.
42. Antti Salovaara, Kristina Höök, Keith Cheverst, Michael Twidale, Matthew Chalmers, and Corina Sas. 2011. Appropriation and creative use: linking user studies and design. In *CHI '11 Extended Abstracts on Human Factors in Computing Systems* (CHI EA '11). ACM, New York, NY, USA, 37-40.
43. Corina Sas and Irni Eliana Khairuddin. 2015. 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* (OzCHI '15), 338- 342. http://doi.acm.org/10.1145/2838739.2838821
44. Corina Sas, Steve Whittaker, Steven Dow, Jodi Forlizzi, and John Zimmerman. 2014. Generating implications for design through design research. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems* (CHI '14). ACM, New York, NY, USA, 1971-1980.
45. Larry Schweikart. 1991. U.S. commercial banking: a historiographical survey. *Business History Review*. 65 (Autumn): 606.
46. Evander Smart. 2015. Top 10 Countries in which bitcoin is banned. Retrieved June 10, 2016 from https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/
47. Melanie Swan. 2015. *Blockchain blueprint for a new economy*. O.Reilly, California.
48. Tether. White paper. Retrieved September 19, 2016 from https://www.weusecoins.com/assets/pdf/library/Tether%20Whitepaper.pdf
49. The Law Library of Congress. 2014. Regulation of bitcoin in selected jurisdiction. Retrieved June 10, 2016 from https://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf
50. UK Government. 2016. Distributed ledger technology beyond block chain. Retrieved June 10, 2016 from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
51. Randall L. Wray. 2012. Introduction to an alternative history of money. *Levy Economics Institute Working Paper*, 717.
52. David Yermack. 2013. Is bitcoin a real currency? an economic appraisal. *NBER Working Paper19747*.
53. Suraya Zainuddin. 2016. The complete guide to bitcoin scams. Retrieved June 10, 2016 from https://www.coingecko.com/buzz/complete-guide-to-bitcoin-scams?locale=en
54. Adam Vaziri Zanjani. 2014. Bitcoin Exchanges as Payment Institution. Retrieved September 16, 2016 from http://neopay.co.uk/site/wp-content/uploads/Diacle-Bitcoin-Regulation.pdf