Exploring Trust in Bitcoin Technology: A Framework for HCI Research

Corina Sas
Lancaster University, UK
School of Computing and Communications,
Institute for Social Futures
corina@comp.lancs.ac.uk

Irni Eliana Khairuddin
Universiti Teknologi MARA, Malaysia
Faculty of Information Management
irnieliana@salam.uitm.edu.my

ABSTRACT
Bitcoin is a crypto-currency which differs in several ways from the traditional use of money. It does not require an individual name but digital wallet IDs, which makes it more private. Bitcoin technology currently lacks protection with respect to monetary transfers, and its structure is not endorsed by the governments. Yet, understanding the concept of trust is fundamental to Bitcoin technology and digital currency economy. This paper offers a review of relevant work on cryptocurrency and trust in HCI, and critically examines its value in understanding the issues of trust in Bitcoin technology. Several limitations of the current theories and models of trust are identified, and a research framework is proposed to explore the specific trust challenges raised by the Bitcoin technology.

Author Keywords
Bitcoin technology; trust.

ACM Classification Keywords
H5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous.

INTRODUCTION
Issued in 2009 by an anonymous entity (Rogojnu and Badea, 2014), Bitcoin technology has become a leader in peer-to-peer crypto-currency (P2P foundation, 2015). It uses nodes of a peer-to-peer network with the purpose of keeping track of transactions, and cryptographic algorithms to provide core security functions (Bitcoin Wiki, 2011). In the Bitcoin network, money is not printed, but *mined*, through widely distributed computing power (Bradbury, 2013). Miners create Bitcoin in a controlled way by running dedicated programs. According to Kervick (2014), Bitcoin architecture differs significantly from prior electronic payment systems, and potentially lacks trust. Bitcoin technology operates through electronic transactions and poses interesting tensions regarding the issue of trust. On the one hand, its open source, decentralized architecture is open for scrutiny. On the other hand, Bitcoin operates under the premise of anonymity: although the transactions under each individual Bitcoin address are publicly archived, the identity of the owner of the address remains undisclosed. Transactions are considered anonymous because nothing ties individuals or organizations to the accounts that enable online transactions.

OzCHI '15 , December 07 - 10 2015, Melbourne, VIC, Australia
Copyright © 2015 ACM 978-1-4503-3673-4/15/12... $15.00
http://dx.doi.org/xx.xxxx/xxxxxxx.xxxxxxx.

While most of the academic work on trust in Bitcoin technology has taken place in cybersecurity and cryptography areas, a user-centered approach to the exploration of Bitcoin has been limited. We argue that a richer understanding of the issue of trust informed by Bitcoin users is important. This paper offers a review of relevant work on money and trust in HCI, and critically examines its value in understanding the issues of trust in Bitcoin technology. The main contribution of this paper is the development of research framework to explore the specific trust challenges raised by the Bitcoin technology. The following section offers a review of the main models of trust. Then we introduce our research framework, and apply it to identify the challenges around trust in Bitcoin technology.

Trust and Digital Currency in HCI
While trust has been a research area benefiting from long-term HCI interest, the issue of digital currency has just starting to capture scholars' attention. In a CHI 2014 workshop focused on financial interactions and digital currency (Kaye, 2014), 12 position papers have focused on issues such as finance, commerce, financial literacy, money democracy, emotions and aesthetics.

Ferreira et al. (2015) have explored user experience with Bristol Pound (£B), a local complementary currency used in Bristol, UK. Authors run a survey with about 200 users on how people conduct mobile phone transactions via SMS, their motivations and challenges for using this currency. Study findings highlighted the payment's unpredictable and slow qualities and their value for strengthening social connections through ludic interactions, as well as increased mindfulness about their practice of purchase and consumption. This underlies the paradox of how a technology lacking trust, allows for strengthening the social trust between the actors involved in transactions, leading in turn to a more cohesive community. The study has also emphasized that Bitcoin technology may benefit from leveraging such face to face social connections in small communities to mitigate the challenges of slow, unreliable transactions.

In a critique of alternative and complementary currency and exchange paradigms, Carroll and Bellotti (2015) have discussed four technological innovations: local

currencies, timebanks, cryptocurrencies, and microenterprises. In particular, they have highlighted the value of cryptocurrency like Bitcoin for individual's privacy and control potentially subverting centralized governmental and financial institutions. Authors have placed this critique in the current global economic context, whose challenges may well benefit from such novel, money centered design and technologies, as a rich space for CSCW and HCI communities to engage with.

With respect to trust, we start by introducing key models and properties. Trust has been described as the subjective belief in the character, ability, strength, reliability, honesty or truth of someone or something (Grandison and Sloman, 2000). In their seminal model of mechanisms of trust, Riegelsberger et al. (2005) described trust warranting properties using the distinction between contextual and intrinsic properties. Their contextual properties consist of temporal, social and institutional embeddedness which are more relevant in the first interaction, while the intrinsic properties of the trustee such as ability, norm-compliance and benevolence become increasingly relevant as trust matures through continual exchanges. The multifaceted concept of trust has been explored across a large range of interactive systems, and consistent findings have shown the distinction between technological, social, and institutional trust (Misiolek, 2002; Lippert and Swiecrz, 2005; Leppanen, 2010).

Technological Trust

The technological dimension of trust consists of individual perceptions and assessments of technology-related trust issues (Leppanen, 2010). The technological trust can be better understood in the light of its three attributes: advantage to use, expectation of technology usability, and perception of user's skills. The *advantage to use* refers to the needs for implementing a technological system that will increase task performance (Goodhue et al. 2006).

Expectation of technology usability has been defined by Davis (1986) in terms of user's initial presumption on what using the technology will be like. Usability can also be seen as a set of objectives and guidelines for system designers and software developers to create devices and applications that take minimal effort for the users to use. For example, Nielsen (2000) proposed guidelines for enhancing individual trust in website by assessing usability in contrast to the risk of making online transactions. *Perception of user skills* capture individual's perception of his or her capabilities and motivations to use a computer or a technological system (Nielsan, 2000).

Social trust

Social trust has been defined as the feeling of the good disposition of the other (Castelfranchi and Falcone, 2001). Leppanen (2010) also identified four key concepts of trust including disposition to trust, perceived trustworthiness, situational factors, and shared attributes which we further outline. *Disposition to trust* depicts the trustor's own willingness to be dependent on others, further determined by a trusting stance and faith in humanity (McKnight et al., 1998). It has been argued that the disposition to this goodwill arises from positive trust-concerning exchanges with people, which lead to a positive general belief on the mankind. Boon & Holmes (1991) also discuss how individual's disposition towards trust sets the expectations for trustworthiness in general. Hence, personal, first-hand positive experience towards a new context is paramount in building up the disposition to trust. *Perceived trustworthiness* has been defined as the expectation that another party will perform a particular action (Mayer et al. 1995; Rousseau et al., 1998). This is an important concept which relies on distinct categories of beliefs such as benevolence, competence, honesty and predictability (McKnight et al., 1998). *Situational factors* are those targeting the context of the organization (McKnight et al., 1998). Moorman (1993) and Purser (2001) argued for the importance of the situation where trust formation takes place. *Sharing attributes* with the trusting partner is crucial in building trusted relationship (Hupcey et al., 2001). These include the importance of positive past exchanges that has been emphasized in Boon and Holmes's model (1991) describing the continuous nature of the shared experience. According to this model, both short- and long-term exchanges can benefit from shared attributes of trust.

Institutional Trust

Institutional trust is defined as the party being initially willingly vulnerable to the counterpart's action (Mayer et al., 1995). It can be described through power relations, and organizational structure. *Power relation* becomes important for trustworthiness in social relationship where an individual has a position of power for decision making in an organization (Tyler and Degoey, 1996). Trust in *organizational structure* reflects the importance of hierarchical relationships across the organization (Kramer, 1996). In McKnight's (1998) trust model, the organizational trust is explained through the system of rules and regulations governing each activity in the organization. There have also been attempts to conceptualize trust in decentralized systems. For example, Gutscher's (2007) trust model integrates public key authenticity verification to evaluate arbitrary trust structures which allow multiple keys per user. It also enables the signer of trust certificate to limit the length of the trust chains and to define the semantic of trust. This trust model consists of four building blocks. Two basic blocks define the existing trust and authentication relations together with inference rules for combining them. The other two blocks describe representations of trust values and how to compute them for trust relations.

Blaze et al. (1996) address the issue of decentralized trust management through four principles such as unified mechanism, flexibility, locality of control, and separation of mechanism and policy. The unified mechanism holds the policies, credentials and relationships for network application security, while the complex trust relationship falls under the flexibility principle. Locality of control supports the trust of relationship across the community, while the separation of mechanism policy supports control of the verifying credentials of the applications.

The trust concepts, models and principles described above either fail to address trust in decentralization

systems or address it from the sole perspective of users of such systems. Bitcoin is not only a decentralized system but a grassroots driven technology involving multiple stakeholders. Thus, it offers a unique perspective to explore the development of trust within and across these stakeholders, together with its most challenging and promising issues. A deep understanding of these trust issues in Bitcoin technology may in turn challenge some of the assumptions underlying our current models of trust.

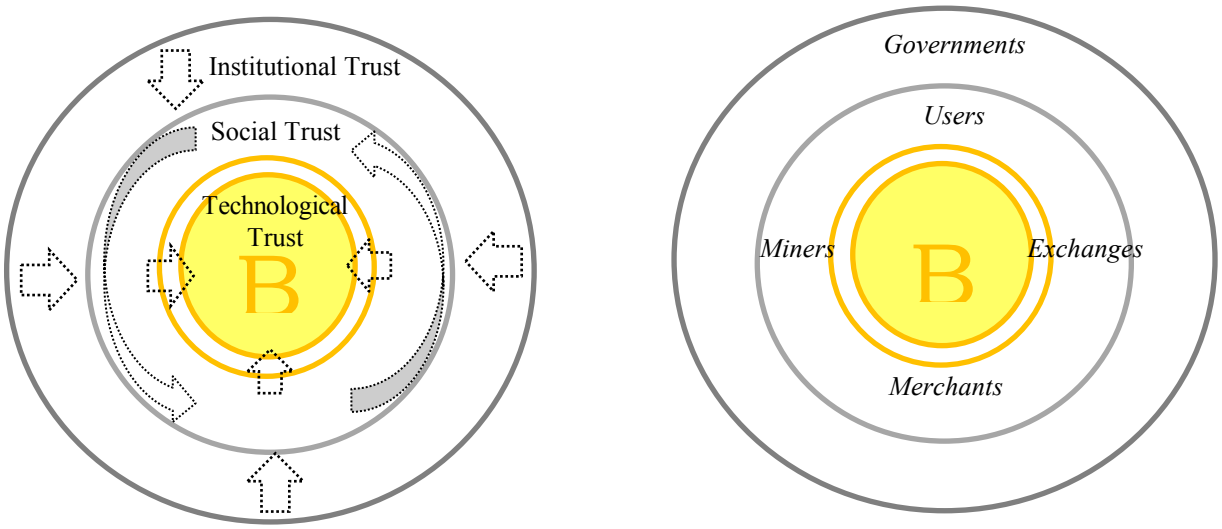

Figure 1: Research Framework for Exploring Levels of Trust in Bitcoin Technology (left) and across Stakeholders Groups (right)

RESEARCH FRAMEWORK

We now propose a research framework (Figure 1) which integrates key aspects of trust from HCI literature, with the main challenges posed by Bitcoin technology, to ensure the exploration of trust across all the Bitcoin stakeholders. The framework places Bitcoin technology at its center, and highlights how different stakeholders are involved in shaping the three different levels of trust. We define *technological trust* as people's trust in Bitcoin technology experienced before, during, and after engaging in online transactions. This could include users' trust that their Bitcoin account is secured and cannot be hacked, or payees' trust that the transfer is authorized.

Social trust is the trust that Bitcoin stakeholders develop between each other. This trust is enlisted for each type of exchange occurring across (and within) different categories of stakeholders. For example transactions involving purchase of goods enlist trust between users and merchants. Upon completion, these transactions require miners' authorization, so both users and merchants need to trust the miners for completing their job. At the same time, selfish miners can raise issues of trust among miners (Eyal and Sirer, 2014). Social trust between users/merchants and exchangers can be also problematic[1]. We argue that because of its decentralized nature, the classic definition of institutional trust does not apply to Bitcoin. However, there is a higher authoring to which Bitcoin technology is requested to be accountable, namely governmental institutions. We define *institutional trust*, the trust of governmental institutions in Bitcoin technology. The main issues here relate to money laundry and deflation.

Applying the Framework to Identify Trust Challenges

We now explore how the framework can be applied to identify important trust issues which deserve stronger HCI engagement. We should note that there is limited empirical work exploring the experience of using Bitcoin and the issues of trust surrounding it. First we start by describing the Bitcoin stakeholders, grouped by Shcherbak (2014) in four categories: users, miners, exchanges and merchants. *Users* are people who use Bitcoin to buy goods and services from Bitcoin merchants. *Merchants* are businesses which accept Bitcoins as medium of exchange for goods and services and are connected to the Bitcoin network. *Exchanges* are the providers of online trading platforms where the registered members can exchange their Bitcoins for traditional currency and vice versa. *Miners* are those Bitcoin stakeholders who can record transactions (and collect reward) after they successfully solved crypto-puzzles (Eyal and Sirer, 2014).

Users' Trust in Bitcoin

One specific challenge pertaining to users is their limited knowledge of how Bitcoin technology works and how they need to protect their bitcoins. Keeping bitcoins on one's computer involves security risks similar to keeping large sums of cash in one's physical wallet (Bitcoin Wiki, 2011). Although Bitcoin is decentralized and at large has no single point of failure, it is nevertheless susceptible to a form of denial of service (Quora Forum, 2011) or double-spending attack (Karame, 2012).

Merchants' Trust in Bitcoin

Merchants' trust is challenged by their limited knowledge about buyers, and whether their payment will be received in time or at all (Shcherbak, 2014). They also lack the

[1] Manhattan, U. S. Attorney Announces Charges Against Bitcoin Exchangers, Including CEO of Bitcoin Exchange Company, For Scheme To Sell And Launder Over $1 Million In Bitcoins Related To Silk Road Drug Trafficking. 27.01.2014. *URL: http://www. justice. gov/usao/nys/pressreleases/January14/SchremFaiellaChargesPR. php*.

ability to track reliable buyers with whom they have previously engaged in positive transactions.

Impact of Miners' and Exchanges' on Bitcoin Social Trust

We know little about the trust challenges faced by these stakeholders. However, exchanges are crucial in supporting users' and merchants' trust, and at large the social trust within Bitcoin system. For example, exchanges have no audit process and no verification procedures (Bitcoin Forum, 2010). Equally, although each transaction should be digitally signed and secure after being verified by an unknown miner, we know little about mechanisms trailing miners' competence and integrity. Recent work has shown that the reward structure which incentivize miners to contribute to the system and its decentralized nature, can motivate some miners to circumvent the Bitcoin protocol and mine selfishly at the cost of honest miners (Eyal and Sirer, 2014). This suggests that issues of trust can also develop within the same stakeholder category.

Governments' Trust in Bitcoin

Bitcoin is a protocol promoted as the first peer-to-peer institution, offering alternative to central banks (Abramowitz, 2014). It has been argued that the demand for peer-to-peer transactions can be an indication for the development of trust in Bitcoin (Bitcoin.org, 2014). In this context is useful revisiting the main components of peer-to-peer governance- as a mechanism for institutional trust in Bitcoin: arbitration, trust, bank, business association and public law. For example, peer-to-peer protocols can offer structure through a set of rules for controlling the Bitcoin technology. Peer-to-peer protocol can also be used as a by governments to develop a structured legal framework for Bitcoin technology. In peer-to-peer decision making, arbitration is one way to resolve disputes (Thornburg, 2012). If peer-to-peer arbitration is able to serve decisions, then it could also serve as the foundation for peer-to-peer trust. It would be beneficial for trustee to be able to invest deposited bitcoins to grow their trust corpus (Abramowitz, 2014). However the challenge in crypto currency is there is no mechanism allowing such accounts to own virtual assets. In order to own the assets, there is a need of an intermediary link between virtual and the real world. Indeed a crypto currency bank may able to establish this connection. If the peer-to-peer bank is able to accept bank funds, make investment decisions, and approve expenditures, then peer-to-peer decision making can be used to operate the peer-to-peer business association (Abramowitz, 2014). A significant obstacles to private peer-to-peer institutions, is government hostility (Abramowitz, 2014). Despite lacking trust, peer-to-peer systems can yet produce decisions with a high degree of consensus. This limited form of decision-making inherent in Bitcoin technology could serve as a foundation for more sophisticated types of decision-making mechanisms, allowing legal institutions to be created without the designation of a central authority.

REFLECTION

We now reflect on the value of this framework for shaping future HCI research agendas. We have shown that the challenges to trust are pervasive affecting all Bitcoin stakeholders, albeit in different ways. They are also interdependent, as distinct user groups may have conflicted goals. Not at least, some trust challenges are hidden, i.e., miners' activity is seldom open for scrutiny. We argue that a user-centered approach to the exploration of trust can shed light into the challenges experienced by people using Bitcoin. This is radically different than the current algorithmic approach to trust in Bitcoin. Research supported by our framework can also open up novel design opportunities to address the identified challenges and support trust. For example, one can imagine new class of interactive technologies where trust is captured, materialized and gained or lost through exchanges. This new design space for decentralized interactive crypto-currency technologies may not only support better adoption of Bitcoin technology but also the digital currency economy at large.

CONCLUSION

This paper introduces a HCI research framework arguing for the importance of exploring trust in Bitcoin technology. The framework builds on theoretical perspectives on trust and discriminates between technological, social and institutional trust, mapped against the four identified Bitcoin stakeholders: users, miners, exchanges and merchants. We have used the framework as a lens for identifying the issues of Bitcoin trust, and shown that they are pervasive, hidden and interdependent. The value of this the framework for HCI research agendas has been also discussed.

REFERENCES

Abramowitz, M. (2014). *Peer-to-peer law built on Bitcoin.* Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2573788

Bitcoin Forum (2010). *Bitcoin.* Retrieved from http://bitcointalk.org/index.php?topic=241.msg8874#msg8874

Bitcoin.org (2014). *Choose your Bitcoin Wallet.* Retrieved form http://bitcoin.org/en/choose-yourwallet

Bitcoin Wiki (2011). *Anonymity.* Retrieved from https://en.bitcoin.it/wiki/Anonymity

Blaze, M. Feigenbaum, J. & Lacy, J. (1996). Decentralized trust management. *Proceeding of Symposium on Security and Privacy*. Oakland, California.

Boon, S.D. & Holmes, J.G. (1991). *The dynamics of interpersonal trust: Resolving uncertainty in the face of risk*. In Hinde, R. A. & Groebel, J. (eds.). Cooperation and Pro-social Behavior. Cambridge University, New York. 167–182.

Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud and Security*, 11, 5-8.

Carroll, J.M and Bellotti, V. (2015). Creating value together: The emerging design space of peer-to-peer currency and exchange. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing*. ACM, New York, NY, USA, 1500-1510.

Castelfranchi, C. and Falcone, R. (2001). *Trust and deception in virtual societies*. Norwell, USA.

Davis, F. D. (1986). *A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results.* Doctoral Dissertation. Sloan School of Management, Massachusetts Institute of Technology.

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security* (pp. 436-454). Springer Berlin Heidelberg.

Ferreira, J., Perry, M. and Subramanian, S. (2015). Spending time with money: from shared values to social connectivity. *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing.* ACM, New York, NY, USA, 1222-1234.

Goodhue, D., Lewis, W. & Thompson, R. (2006). PLS, small sample size and statistical power in MIS research. *Proceedings of the 39th Annual Hawaii International Conference.* 8, (4) 202.

Gutscher, A. (2007). A trust model for open decentralized reputation system. *Journal of IFIP International Federation for Information Processing,* 238 285–300.

Grandison, T. Sloman, M. (2000) A survey of trust in Internet application, *IEEE Communcations Surveys & Tutorials* 3(4).

Hupcey, J. E., Penrod, J,. Morse, J. M., & Mitcham, C. (2001). An exploration and advancement of the concept of trust. *Journal of Advanced Nursing*. 36, (2) 282-293.

Karame, G., Androulaki, E. & Capkin, S. (2012). Double-spending fast payments in Bitcoin. *Proceedings Computer and communications security* (pp. 906-917) ACM.

Kaye, J. et. al. (2014). CHI money: financial interactions, digital cash, capital exchange and mobile money. *CHI '14 Extended Abstracts on Human Factors in Computing Systems ACM*, New York, NY, USA, 111-114

Kervick, D. (2014). *Bitcoin evolution towards self-destruction.* Retrieved from http://neweconomicperspectives.org/2014/03/bitcoins-evolution-toward-self-destruction.html#more-7707

Kramer, R. M. 1996. Divergent realities and convergent disappointments in the hierarchy creation: trust and the intuitive auditor at work. In Kramer, R. M. & Tyler, T. R. (eds.) *Trust in Organizations: Frontiers of Theory and Research*. Sage Publications, Thousand Oaks, California. 216-245.

Leppanen, A. (2010). *Technology trust antecedents: building the platform for technology enabled performance.* Retrieved from http://epub.lib.aalto.fi/en/ethesis/pdf/12310/hse_ethesis_12310.pdf

Lippert, S. K. & Swiercz, P. M. (2005). Human resource information systems (HRIS) and technology trust. *Journal of Information Science*. 31(5) 340-353.

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

McKnight, D. H., Cummings, L. L. & Chervany, N. L. (1998). *Initial trust formation in new organizational relationships* .The Academy of Management Review. 23(3) 473-490.

Misiolek, N., Zakaria, N. & Zhang, P. (2002). Trust in organizational acceptance of information technology: A conceptual model and preliminary evidence. *Proceedings of the Decision Sciences Institute 33rd Annual Meeting*: San Diego, California. 1-7.

Moorman, C., Deshpandé, R. & Zaltman, G. (1993). Factors affecting trust in market research relationships. *Journal of Marketing.* 57(1) 81-101.

Nielsen, J. 2000. Designing Web Usability.New Riders, Indianapolis, Indiana.

P2P Foundations (2015). *Definition of Bitcoin.* Retrieved from http://p2pfoundation.net/bitcoin

Purser, S. (2001). A simple graphical tool for modeling trust. *Journal of Computers & Security*. 20(6) 479-484.

Quora Forum. (2011). *How can Bitcoin be hacked?* Retrieved from http://www.quora.com/How-can-Bitcoin-be-hacked.

Riegelsberger, J., Sasse, M. A., and McCarthy, J. D.

(2005). The mechanics of trust: a framework for research and design. *International Journal of Human Computer Studies*. 62(3) 381-422.

Rogers, E. (1995). *Diffusion of innovations*. Free Press, New York.

Rogojanu, A. and Badea, L. (2014). The issues of competing currencies, Case study – Bitcoin. *Theoretical and Economics Journal*, 21(1), 103.

Rousseau, D.M., Sitkin, S.B., Burt, R.S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. A*cademy of Management Review,* 23. 394-404

Shcherbak, S. (2014). How should Bitcoin be regulated? *European Journal of Legal Studies*. 7(1) 46-91.

Tajfel, H. & Turner, J. (1979). *An integrative theory of intergroup conflict.* In Austin, W. G. & Worchel, S. (eds.). The Social Psychology of Intergroup Relations. Pacific Grove, California. 33-47.

Thornburg, E. G. (2012).Going private: technology. Due process and internet dispute resolution: *The Federal Arbitration Act.* 9, 1-16

Venkatesh, V. & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Journal of Management Science.* 46(2) 186-204.