Journal of Information and Knowledge Management (JIKM) Volume 11 Number 2 (2021)

The Algorithm Design for Trust in Peer-to-Peer Bitcoin Transactions on Blockchain

Irni Eliana Khairuddin

Faculty of Information Management,
Universiti Teknologi MARA, UiTM Selangor,
Puncak Perdana Campus, 40150 Shah Alam, Selangor,
Malaysia

Email: irnieliana@uitm.edu.my

Received Date: 1 September 2021
Accepted Date: 22 September 2021
Published Date: 1 October 2021

Abstract. Bitcoin is a cryptocurrency that has created a new revolution in peer-to-peer technology. Built upon decentralised technology known as Blockchain, it supports transparent, fast, cost-effective, and irreversible transactions, without the need for trusting the third-party financial institution. The privacy of Bitcoin users is protected, by the pseudoanonymous transaction. At present, Bitcoin holds the largest market share in cryptocurrency and the Blockchain technology had captured the interest of multi-corporations, such as Microsoft, Dell, and T-Mobile. However, Bitcoins have no legal tender in most and it is even worse with the illicit use by the irresponsible people and the cyber-attacks towards the application. Hence, these are the primary motivation of this study, to design the algorithm for trust in peer-to-peer transaction. The design work was conducted by using a physical blockchain kit, namely BlocKit with 15 Bitcoin Blockchain experienced to explore the opportunity to develop the algorithm.
Keywords: bitcoin, blockchain, trust, algortihm

1 Introduction

The sophisticated technology of Blockchain was designed with core characteristics such as transparent and decentralised that support the users' trust towards the technology (Sas and Khairddin, 2015). However, the highlighted issue from the finding by Sas and Khairddin (2017) is on the social trust among the users in conducting peer-to-peer transactions for the exchange of Bitcoin and physical goods or fiat money. Although Bitcoin transactions are transparent on Blockchain, the process of sending the physical goods or fiat money is not. This leads to issues of trust such as dishonest trader, scams and fraud. Mitigating actions among users have been taken such as by trading with authorised exchanges, socially authorised traders, reputable individual traders or de-anonymised individual traders. This study argues that there are opportu-

nities to mitigate the issue on Blockchain. In making the efforts to explore the design for trust on Blockchain, it is hard to understand and communicate with the complex technology of Blockchain. Thus, the construction of BlocKit (Khairuddin, Sas and Speed, 2019) offers an exploration to verify the abilities of this DIY kit for design as well as to support the understanding of Blockchain.

In this study, BlocKit was used to design the algorithm for trust in bitcoin transaction among the users. The participants were presented with 11 objects of BlocKit with the aim of addressing the following research questions:

- how can trust among Bitcoin users be materialised and designed for through BlocKit?
- what are the requirements to design for trust among Bitcoin users?

The findings describe the Bitcoin Blockchain experienced users' experience in interacting with the kit as a medium of communication to design the trust for bitcoin on blockchain. In the light of this evaluation, the findings discussed the suggestion for the design for trust as well as their suggestions for the principles and requirements to design for trust in Bitcoin users.

2 Literature Review

Trust between People and Technology

According to Misiolek et al. (2002) technology trust research should include the three distinct dimensions of trust: social trust, institutional trust and trust in technology. Leppanen, A. (2010) also agree that there three area, if considered as abundantly available resources, contribute to a higher level of technology trust. Lippert and Swiecrz (2005) also utilize a similar three-tier division of areas that influence an individual when technology trust relationship is considered. Their models dividing the technology trust into user, organizational and technological categories both confirms Misiolek et al.'s (2012) structural approach validity and also allows for more in-depth overview of the areas. Technology plays a crucial role in assessing technology trust. The technological dimension antecedents rise from the individual perceptions and assessments of technology-related issues and not so much from the technological innovation being the object for trust.

The technological trust consists of individual perceptions and assessments of technology-related trust issues (Leppanen, 2010). It 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, Lewis, & Thompson, 2006). The expectation of technology usability has been defined by Davis (Davis, 1989) 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 to use. For example, Nielsen (Nielsen, 2000) proposed guidelines for en-

hancing individual trust in website by assessing usability, in contrast to the risk of making online transactions. The perception of user skills captures each individual's perception of his or her capabilities and motivations to use a computer or a technological system (Nielsen, 2000).

The prevalent model of trust related to trust between people and technology is the model of online trust. Corritore and colleagues (Corritore, Kracher, & Wiedenbeck, 2003) identified three trust factors: user perceptions 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 (the expectation that technology will act consistently based on past experience), and reputation (recognised 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 that of Davis (Davis, 1989).

Trust in Bitcoin Blockchain Technology

Issued in 2009 by an anonymous entity (Rogojanu & Badea, 2014), Bitcoin technology has become a leader in peer-to-peer crypto-currency, allowing secure transfer and exchange of digital tokens in a distributed and decentralised manner (Nakamoto, 2008). Bitcoin can be exchanged for other national fiat currencies at the agreed market rate (Coin Desk, 2019) through online marketplaces into a digital wallet. In addition to money, the exchange can also be done for goods and services, or use the Bitcoins to buy goods or properties (Göbel et al., 2015). At present, Bitcoin is a leader among more than 2000 peer-to-peer currencies on the market (Coin Market Cap, 2019) and experts have foreseen that Bitcoin users will reach almost 200 million by 2024 (Young, 2017).

In the Bitcoin network, money is not printed, but mined through widely distributed peer-to-peer network computing power in a controlled way by the miners running a dedicated program in their computer system (Bradbury, 2013). The miners' job is to run the program to record the Bitcoins transactions from one user to another user. Those transactions will be recorded in a publicly distributed ledger called Blockchain (Swan, 2015). In a Blockchain ledger, the set of Bitcoins' transactions are publicly distributed throughout the peer-to-peer nodes across the network. The uniqueness of this underlying technology for Bitcoin is it allows for secure and transparent transactions while protecting the identity of transaction's parties (Nakamoto, 2008). Transactions are considered pseudoanonymous because although the transactions are publicly archived under an individual's Bitcoin address, the identity of the owner's address remains undisclosed. These processes in Bitcoin network are decentralised and supported by multiple stakeholders.

Sas and Khairuddin (2015), have identified the different stage of trust of for different types of bitcoin stakeholders, users, miners, exchanges and government towards the technology. The most crucial trust issue in the bitcoin transaction is related to users' trust which involves people who has limited knowledge of the how bitcoin technology works and the risk of keeping bitcoin on the wallet (Sas and Khairuddin, 2015). Furthermore the trust among the users are also been highlighted (Sas and

Khairuddin, 2017). This is due to the peer-to-peer transaction that have been conducted by the users, which it opens spaces for scams.

Materializing of Bitcoin Blockchain with BlocKit

Blockchain is a disruptive technology which has significantly challenged assumptions that underpin financial institutions and has provoked innovation strategies that have the potential to change many aspects of the digital economy. However, because of its novelty and complexity, Blockchain had challenged people's understanding of its inner working. Due to its complexity, different modalities have been explored to communicate the principles of the Blockchain, and support their understanding and learning primarily through visual representations in the form of infographics (Cartwright, 2018) or (The Guardian, 2014) video. In contrast, the value of physical objects for communicating about Blockchain has been limitedly explored, with some preliminary work suggesting the value of Lego blocks for Blockchain experts and novices to communicate and describe its entities (Maxwell et al., 2015).

BlocKit is a physical representation of Blockchain infrastructures that was built based on the entities properties, embodied cognition theories and material centred-design. It consists 11 important bitcoin blockchain elements which includes wallet, bitcoin, consensus rules, private key, public key, memory pool, block, miners and blockchain ledger (Khairuddin, Sas and Speed, 2019). The BlocKit was constructed as a new methodological approach to design on the Blockchain, in particular, with the aim to externalize the complex Blockchain infrastructure to facilitate the users' understanding and communication in the exploration to design for trust in Blockchain (Khairuddin, Sas and Speed, 2019)

3 Research Method

In this study,15 Bitcoin Blockchain experienced users, 12 males, 3 females, and (mean age 29, range 21-39) were recruited for a workshop. All participants had at least 2 years of engaging in Bitcoin transactions: 9 had between 2 and 3 years, 4 had between 4 and 5 years, 2 had more than 6 years. All participants have at least graduate education, i.e., 6 BSc, 7 MScs, and 2 PhD Participants were recruited through the mailing lists of two universities, and through a local Bitcoins meetup group.

The workshop involving the use of the BlocKit (Khairuddin, Sas and Speed, 2019) that aimed to explore how they materialise trust in bitcoin transaction. The study started by asking them how Bitcoins transactions take place on the Blockchain after the study showed them the BlocKit's 11 objects to simulate transactions while thinking aloud.

In the second part, the study provided two round-shaped pieces of clay, one green and one red representing trust and distrust token, respectively, and asked participants to include them in Bitcoin transactions while thinking aloud. The whole workshops lasted between 60 and 90 minutes, were video recorded, and fully transcribed.

Data analysis involved a hybrid approach with concepts from the deductive coding and new ones emerging from the empirical data, contributing to the inductive coding

(Fereday & Muir-Cochrane, 2006). The coding list was iteratively revised in the light of the interview data, as new codes emerged under the themes of properties of Blockchain's entities, and their materialisation.

4 Research Findings

Designing for Trust for Bitcoin Blockchain Transaction with BlocKit

The anonymity principle is central to design for trust in the Blockchain protocol, which in turn raises significant trust challenges for both users and miners (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017). Hence, designing for trust on Blockchain is an important challenge to be explored with experienced users. In the second part of the workshop, the study provided tokens to explore experienced users' design solutions for materialising the flow of trust on Blockchain. Findings indicate three themes consisting of rewarding honest transaction partners with trust token, penalising dishonest ones with distrust tokens, and accounting for the mining fee associated with the flow of trust. Participants iteratively identified six ways of materialising trust flow on Blockchain by (i) placing the token of trust within the Bitcoin transaction (P1, P3, P7), (ii) ensuring 2 way transparent transactions (P1, P2, P4, P5, P7), (iii) centralised mediator (P2, P4, P6, P8, P10, P15), (iv) 2-of-2 multisignature address (P3, P4, P5, P6, P8, P9, P11, P12, P13), (v) 2-of-3 multisignature address (P8, P9, P10, P11, P12, P13, P14, P15), and (vi) crowdsourced, decentralised mediator (P8, P9, P10, P11, P12, P13, P14, P15).

Each of the first five solutions was discarded as they challenged Blockchain's assumptions of decentralisation, unregulation, or anonymity. The first solution was enacted by placing the green clay trust token together with the other objects representing a transaction, i.e., Bitcoin clay, sticky notes with wallet address and signature, but failed to recognize that Bitcoin transactions are often accompanied by transactions of fiat currency or goods in the physical world, whose trust is problematic to capture on Blockchain (Sas & Khairuddin, 2017).

The second solution resembles the existing Omni layer approach (Omni Layer, 2017) allowing two or more parties to trade transparently over the Bitcoin Blockchain, but fails to acknowledge the asynchronous nature of 2 way transaction, and that in case of fraud, transparency is not sufficient to reverse a fraudulent transaction nor to sanction the fraudulent user.

The third solution suggests centralised mediator: *"both parties have to commit […] and when both money and Bitcoins arrives in here, both will get it at the same time"* [P4], and participants represented it through the object of a transparent container holding all the objects involved in a transaction. This solution resembles the current escrow or exchange services, addressing the asynchronous problem of two-way transaction, but failing to account for the decentralisation, unregulation, or anonymity principles of Blockchain. Indeed, escrows prevent fraud by requiring both parties to register their identity (Local Bitcoin, n.d.).

One way to address the risk of de-anonymisation is through 2-of-2 multisignature address which requires both parties to co-sign for a newly created third address to temporarily hold the Bitcoins before released to the destination wallet (Electrum,

2017; MultiChain, n.d.). This solution fails in case of dispute or fraud, and therefore 8 partisans suggested the 2-of-3 multisignature where a third party assists the dispute by signing the transaction (Lerner, 2015; WeiDex, n.d.). This solution was represented by placing 2 sticky notes with a different wallet address in the novel transparent container representing the third address: "*you can have it signed as two of two to receive the Bitcoins and trust token). […] However, if you have a disagreement then it's obviously stuck in here [and you need a 2-of-3 signature]"* [P12].

To address this limitation, more than half of participants proposed placing the transaction in a smart contract and the novel approach to use a crowd-sourced mediator or witness for the contract. To represent it, participants extended the previous transparent container with 2 sticky notes, by placing an additional sticky note on the transparent container: "*you can add another user that is randomly assigned in a contract to validate the transaction […] and signed by 2-of 3 […] At the end of a successful transaction, this trust token can be sent by the buyer and seller (mimic the movements of green clay from buyer to seller, vice versa) […] and appreciation token to the other user who helps to witness the transaction"* [P9]. This is a novel design solution, extending smart contracts and multisignature accounts (Horda, 2018; Lerner, 2015; Matzutt et al., 2018) which have started to be used on Ethereum Blockchain (Horda, 2018) for instance for decentralised exchange such as WeiDex (WeiDex, n.d.). However, the development for a fully decentralised exchange for Bitcoin Blockchain is limited (Cuen, 2018), as it also the idea of trust token and witness token. In the case of dishonest transaction partner, the witness "*needs to take charge to verify the transaction by requesting the agreed quality of the offline transaction's proofs as stated in the contract from both seller and buyer. […] the witness will decide whether to move the Bitcoins (*from multisignature wallet*) to the buyer's or reverse it to the seller's wallet […]. It also reflects the increments of trust and distrust token for both wallets as specified in the contract"* [P10].

All participants agreed on the associated cost related to trust, suggesting that both parties should have an agreement regarding the fee, before enacting any transaction. In addition, 8 participants also suggested a small fee for incentivising the witness.

Principles to Design for Trust of Blockchain

Findings also suggested design principles for trust in peer-to-peer Bitcoin transactions. Findings identified four important suggestions such as a valid contract, transparent transactions, decentralised mediator, and reputation token which are further described.

Valid Contract

Prior to enacting a peer-to-peer Bitcoin transaction, an agreement between the seller and buyer to decide on the details of the transaction is vital. Indeed, our previous findings reported fraud cases caused by one of the parties not fulfilling their promise (Sas & Khairuddin, 2017), One way to overcome this risk, is by creating a valid agreement between seller and buyer before enacting the transaction: "*write a proper contract for the transaction* […] *so you don't have to trust them (buyer) and they (buyer) don't need to trust you as the seller, it is because the contract says everything*

and it is valid" [P13]. Hence, with a valid agreement, both buyer and seller are bonded with the contract. The suggestion to create a contract is an extension to the usual practice by making the negotiation and agreement. These include their details of bank account for fiat money and wallet address for receiving Bitcoins. But those are just word-of-mouth and there is no guarantee they will follow the agreements. By having an agreement in a contract, they are not able to escape as they have to agree to bear the penalties if they commit frauds. This mentioned by 6 participants: "*if let's say any of them break the contract, the Bitcoin is sent to the honest party* […] *or any other punishments they can write in the contrac*t […] *and there is no way to run* (from fulfilling the contract)" [P13]. Although there is no central authority that governs the transaction, by having a valid contract will permit a trustless transaction between both parties. It is because the social trust among buyer and seller is no longer required as the transaction is protected with the rules in the contract that have been agreed by them. In the framework on the mechanic of trust that facilitates the trust between people with mediated technology, which can be classified as institutional trust (Riegelsberger et al., 2005).

Transparent Transactions

In normal practice for peer-to-peer Bitcoin transactions, it will begin with one party (buyer) sending money followed by the seller enacting the Bitcoins transaction (Sas & Khairuddin, 2017). Regarding this, more than half of the participants described the possibility of fraud facilitated by this common practice: *"(the) buyer can claim, he has sent the (fiat) money although he actually did not and (the) seller can also cheat by claiming that she did not receive the buyer's (fiat) money even though she did"* [P8]. Fraud can also happen in the transactions between Bitcoins exchanged for goods: *"Let's say you want to buy a product from a Bitcoin merchant. You are lucky to get the correct product […] but how if they fool you?*[…] *and yet you have sent them your Bitcoins?"* [P1]. Such challenges contribute to distrust towards the anonymised peer-to-peer transactions among Bitcoin users.

In order to mitigate these issues, 6 of participants suggested to create the rules for fair and transparent transactions between the seller and buyer through a multisignature wallet: "*it begins with the seller sending the Bitcoins to a created multisignature wallet address. Then when the buyer sees the Bitcoin is available in that wallet address, he will send the money to the seller's offline account and immediately sign on that multisignature wallet to request to release the Bitcoin. […] Once the seller received the money in the bank, he or she will also sign on the wallet, and the Bitcoin will be released to the buyer's wallet"* [P11]. This quote mirrors that Bitcoin's transaction should begin by sending Bitcoin to a multisignature wallet address. Hence, this will create a fair and transparent transaction, as both parties have access to the Bitcoin multisignature wallet as well as the control over it. In other words, once the Bitcoin is sent to the multisignature wallet, it will not able to move to another wallet address, unless it gets the approval or signature from both seller and buyer. This algorithm will facilitate the trust between the buyer and seller in the credibility of the systems assisting peer-to-peer transaction in such decentralised, unregulated infrastructure, such as Blockchain (Corritore et al., 2003).

Decentralised Mediator

Findings also indicate a challenge in facilitating the transaction between buyer and seller through multisignature wallet: *"However if you have a disagreement then it's obviously stuck in here (multisignature wallet)* [P12]. Such view is shared by 6 participants, and they suggested an interesting solution to mitigate this issue: *"Another wallet address (Bitcoin user) from the network can be randomly assigned to validate the transaction"* [P14]. This reflects on *crowdsource mediator functions* that help to validate the peer-to-peer transaction. This, in turn, made the multisignature wallet now consist of three parties: seller, buyer and the crowdsourced mediator or also known as a witness for the transaction.

This is a novel finding as unlike most of the Bitcoin exchanges' wallet, they embedded escrow service in their system. This service acts as the third party for buyer and seller's transactions by temporarily holding their money and Bitcoin in the escrow's account then disburse to the respective wallet and bank account for the transactions. The similarity of escrow service and crowdsourced mediator is that both are the mediator for Bitcoin and offline counterpart transactions. But the difference consists of being centralised and decentralised for the latter mediator. This in turns shows that the use of mediator is essential to facilitate trust in a transaction. In the framework of trust, the role of decentralised mediator supports the social trust for the peer-to-peer Bitcoin transactions (Riegelsberger et al., 2005).

Reputation Token

Blockchain is originally designed with the anonymity concept. However, due to the issue of trust, people tend to de-anonymise themselves for enacting peer-to-peer transactions (Sas & Khairuddin, 2017). In this study, findings suggest to build a wallet reputation system: *"although the wallet is anonymous, the number of ratings received for that particular wallet, can reflect the credibility of the user (owner)"* [P10]. Seven participants shared similar opinion. The rating scores of the wallet will indicate the credibility of the wallet's owner which the identity of the owner is remain anonymised. However, there may be an issue of one person handling more than one wallet and keeping on sending the rating to each of their accounts, as concerned by most participants. In order to mitigate this issue, seven participants suggested the initial date of the wallet creation is visible: *"the reputation for the wallet can also be seen on the date of the wallet created. So people will know how long the wallet exists and (will be) able to compare with the number of transaction made and reputation level"* [P10]. This reflects that the length of the presence of the wallet and the rating scores could also contribute to the paradigm of trust.

The findings further highlight the importance to know the regularity of transactions in between the same wallets, as mentioned by 5 participants: "*there should not be a limitation of transactions in between two wallets, but create a mechanism to show the sender of each trust token received. So people can see the frequency of transactions between two wallets"* [P15]. This transparent reputation system is essential to monitor such transactions.

Meanwhile, for the new user, there is also a possibility for them to build the trust associates from a wallet: *"Yes the problem will be for the new user. But I think they got*

to start with a small amount I suppose […] which is similar to other reputation systems […]. The idea is to have the reputation sign that you can link with your wallet id" [P12]. For a new user, if they perform an honest transaction, the trust token will be rewarded to her wallet. The tokens gained should also be accompanied in a form of ratio, as mentioned by more than 7 participants: *"The new account will start from zero tokens. Let say for one trusted transaction, she will get 1 token, then maybe next transaction she gets another trust token. But for the third transaction, she gets distrust token. So it will calculate the average of trust token that she received in a form of percentage for instance"* [P14]. A trust ratio associated in a wallet should reflect on total trust and distrust token gained by the user.

Participants also suggested ways to incentivise the decentralised witness of a transaction: *"the buyer and seller can also send him* (witness) *a witness token as an appreciation for them. This token will be showed in his wallet and visible to others. This will give an added advantage to the witness to build his reputation"* [P8]. Referring to the trust model, the element of reputation is one of the principles for the trust system that is supported under the social trust dimension (Riegelsberger et al., 2005).

The Requirements for the Principles to Design for Trust Bitcoin Blockchain Transaction

In this section, the study will describe the capabilities of Blockchain to build the identified principles to design for trust transactions. The findings had identified four important characteristics of Blockchain which are storing information in Blockchain, smart contract, multisignature wallet and low-cost transaction that will be further described in this section.

Storing Information in Blockchain

One of the unique characteristics of Blockchain is the ability to store valid information as well as to make it transparent for users (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017; Swan, 2015). Other than storing the Bitcoins transactions, Blockchain is also capable to store other types of information, as mentioned by seven participants: *"you can send Bitcoins and include some arbitrary information with the transaction […] and it will be recorded in the Blockchain. […] For instance this token* (trust token*) or whatever information can be recorded in the Blockchain"* [P3]. This quote reflects the ability of Blockchain to be the underlying technology for the decentralised reputation system for the Bitcoin transaction. Moreover the unique characteristics of Blockchain for being decentralised, irreversible and permanent transactions (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017; Swan, 2015) enable the development of reputation systems to be reputable compared to the ordinary reputation systems in most e-commerce website: *"trust could be seen as a form of value that can be exchanged and enhanced people's trustworthiness. So, I think somehow being able to use the Blockchain to do that is interesting, because again, you can't tamper with it like eBay that you can affect the rating"* [P5]. By building a reputation system in the Blockchain, it will enable the process of sending and receiving the reputation tokens to be transparent for not only between the seller and buyer but the entire world. It is

because, decentralisation and transparency are among the core principles of Blockchain (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017; Swan, 2015).

Smart Contract

The details of agreements between seller and buyer could be sealed in the form of a valid contract in the Blockchain. Four of the respondents suggested building the contract using the Etherum smart contract: *"Etherum Blockchain has this concept called smart contract, so a smart contract is essentially a self-executing piece of code which only executes when certain conditions are met. For example, after the transaction, you could ask each party for feedback on whether they thought that the transaction went smoothly or […] something was wrong. So, if they both say yes, it went smoothly on the smart contract you could say well this wallet address and this wallet address gets token of trust"* [P6]. This in turns allows the buyer and seller to write their agreements in the smart contract. In the contract, they should state all the related details of the transactions including the agreed selling price, method of offline payment, trust tokens and penalties for being dishonest, such as to receive the dishonest token. The smart contract will automatically set specific computational algorithms to run the contract as mentioned in the quote. Thus, if they both met the details in the contract, the smart contract will execute the contract by sending trust tokens for both and if not, the dishonest will bear the penalty by getting the dishonest token.

Multisignature wallet

Findings also suggest to include the crowdsource validator or witness as a mediator for each transaction. This can be built by using the multisignature features mentioned by two of the respondents: *"Yes, of course, you can add the multisignature function in Blockchain. I know Bitcoin Blockchain has the multisignature and Eetherum also do"* [P9]. This shows that the design of the trust system in Blockchain can be supported with multisignature features that include 3 parties, buyer, seller and witness. The function of multisignature wallet can be found in several exchanges wallet such as Coinbase (Khatwani, 2018). There also some Bitcoin wallet includes administrative mediator, which is centralised in the multisignature wallet to manage disputes (BTC.com, 2017). However, to combine buyer, seller and the crowdsourced mediator for a transaction in the multisignature wallet is a novel design.

Low cost of transaction fee

In order to record contract also trust and witness token in Blockchain, the seller and buyer need to commit a small mining fee, almost ten of the respondents shared this view: *"it costs the transaction, they (buyer and seller) spend a very small amount of money, but apart from that, they can include that kind of token information in that transaction and build their own credibility"* [P3]. The minimum fee for the contract would be worth for the seller and buyer to build their trust reputation for the future peer-to-peer transaction.

Sections 7.21 and 7.22 report on the findings from the workshop with the Bitcoin Blockchain's experienced users on BlocKit. The theoretical and design implications will be discussed in the following section.

5 Research Implications

Principles to Design for Trust in Peer-to-Peer Bitcoin Transactions

The findings advance the theories of trust in HCI (Corritore et al., 2003; Riegelsberger et al., 2005; Sas & Khairuddin, 2015) as well as the trust challenges in Bitcoin transactions (Khairuddin & Sas, 2019; Sas & Khairuddin, 2017) to frame the findings for the principles to design for trust for the peer-to-peer Bitcoin transactions.

In the light of the Bitcoin trust framework (Sas & Khairuddin, 2015) and the technological trust model (Corritore et al., 2003), the findings suggest the principle to design transparent transactions in multisignature wallet is able to leverage users' technological trust. This is important to avoid fraud in the offline transaction. Underlying the uniqueness of the transparent Blockchain characteristic (Swan, 2015) the integration of the design principles and multisignature wallet (Horda, 2018) enable the seller to make the first move by sending the Bitcoin to the multisignature wallet address securely. It is because the wallet is transparent to both parties in the transactions as well as protected by the signature of seller and buyer. Hence the Bitcoin will not be able to transfer to the counterpart's wallet until the offline transactions with fiat money or product are completed. This opposed the usual practice of Bitcoin peer-to-peer transactions that had caused multiple fraud cases (Sas & Khairuddin, 2017).

The principles to design the transparent transaction is supported with a contract between the seller and buyer in the Blockchain smart contract (Horda, 2018) that stand as the legal evidence for the transaction (Huillet, 2018). The evidence in the smart contract did not involve the governmental support but interestingly it can be applied as a valid legislative document. This finding extends dimensions of institutional trust in the Bitcoin trust framework (Sas & Khairuddin, 2015), as it proofs that the user's trust in Bitcoin transaction is not only relying on the government to legalise the transaction but also may depend on the decentralised evidence such smart contract. The similar arguments are used to stand as novel findings for the framework of trust in between users mediating the technology (Riegelsberger et al., 2005).

Findings also indicate novel insights into the social dimension of trust. Instead of applying technology to strengthen the social trust, findings indicate that the decentralised witness could act as the mediator for the transaction between seller and buyer, which replaced the centralised escrow service (Local Bitcoin, n.d.). This has transformed from using technology to mediate trust to the human capabilities as a mediator for trust. Hence this study argues that the decentralised witness is an extension characteristic of social trust dimension in the framework of mechanic trust (Riegelsberger et al., 2005). In addition, the findings also suggest to include the reputation system as one of the principles of trust to support the social trust (Riegelsberger et al., 2005) in peer-to-peer Bitcoin transactions.

The Design of Algorithms for Trust in Peer-to-Peer Bitcoin Transactions

Four principles for designing for trust in peer-to-peer Bitcoin transactions have been outlined by 15 experienced Bitcoin Blockchain users in Study 3: a valid contract, transparent transactions, decentralised mediator, and reputation token. Hence, based on those principles, the design of the algorithms in the Blockchain platform will be further discussed in this section.

The design of valid contract in Ethereum smart contract supported with BTC Relay tool

The Ethereum Blockchain offers a unique tool that allows users to write a set of contract that are automatically executed whenever the conditions in the contract are met (Horda, 2018). In order to execute the contract, users are required to pay a transaction fee in Ether for the miners. However, for Bitcoins transactions, the application of the BTC Relay allows Ethereum smart contracts to securely verify Bitcoins transactions including the contract execution fee that can be paid in Bitcoin instead of Ether (BTC Relay, 2016). The combinations of Ethereum smart contract and BTC Relay are novel design solutions for Bitcoin Blockchain. Meanwhile, as for Ethereum Blockchain, the smart contract has been widely applied in various apps such as CryptoKitties (CryptoKitties, n.d.).

Therefore, the design for trust in peer-to-peer Bitcoins transactions, the agreement between seller and buyer for the transactions of Bitcoins with fiat money or products could also be written in a smart contract. The details of the agreement, such as the selling price, method of payment for offline transactions, and timeframe for the transactions should be included in the contract. Both buyer and seller must also agree on the transaction fees for executing the contract. The smart contract is connected to BTC Relay to verify the payment fees, made by users in Bitcoins. Once the payment is verified, the contract will be executed (*Figure 1)*.

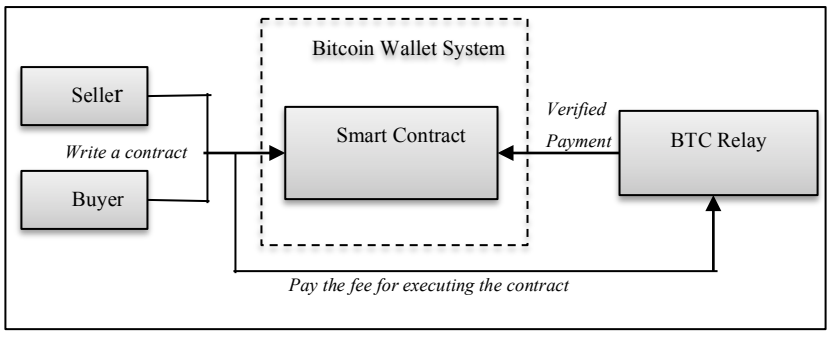

Fig. 1. Algorithm design to create a valid contract for Bitcoin Peer-to-peer Transaction

The design of Bitcoin transparent transactions between buyer, seller and decentralized mediator with multisignature wallet contract

The multisignature wallet has been used in several Bitcoin wallets and exchanges, such as Coinbase and BTC.com wallet (BTC.com, 2017; Khatwani, 2018). The aim of using the multisignature wallet is to provide a transparent mechanism for all parties involved in the transaction. In addition, the Ethereum smart contract could also be linked with the multisignature wallet. Therefore, in order to write and execute a contract, all parties involved in a particular transaction would have the authority to sign the contract. These mechanisms have been applied in several types of system including the system for managing real estate documents (Karamitsos et al., 2018).

In addition, in Bitcoinpeer-to-peer Bitcoins transactions, although the multisignature wallet enables transparent transactions between seller and buyer, who could also write the agreements for the transactions in the smart contract, there are still possibilities of conflicts among the buyer and seller which are beyond the contract. Hence, as suggested by the experienced users in Study 3, together with the buyer and seller, the study included the decentralised mediator in the smart contract embedded with the multisignature (multisignature wallet contract). The mediator is randomly appointed among the owners of Bitcoin wallets. Then the Bitcoin wallet owners that accept the offer to be the mediator will be responsible to witness that particular transaction between seller and buyer as well as to manage the dispute between them. In return, the decentralised mediator will be rewarded with a witness token and for any dispute managed by them, they will get some incentives. This is a novel design solution as currently there are plenty of Bitcoin wallets embedding the centralised administrators to monitor the dispute for each Bitcoin transaction (BTC.com, 2017) in their wallet system, however, there are limited findings for the type of Bitcoin wallet that embed a decentralised mediator in their system (*Figure 2*).

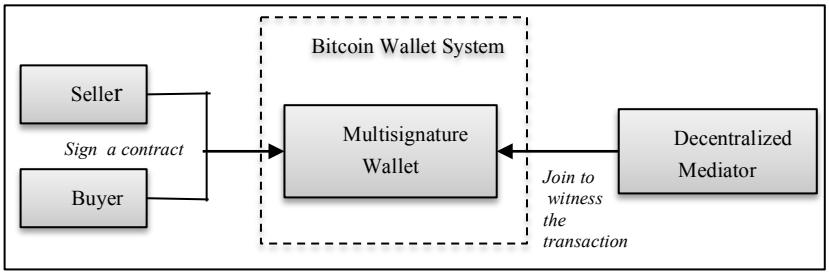

Fig. 2. Algorithm design to create a transparent peer-to-peer Bitcoin transaction with decentralized witness

The design of reputation token in Blockchain ledger

The reputation system management model has been widely applied in various areas such as e-commerce, peer-to-peer system and social networks (Rahimi & Bakkali, 2014). The aim to apply reputation system is to provide the long term reputations records to inspire future interactions, and also to capture feedbacks on present interactions and to allow other users to access the reputation ratings for trust decision (Janiszewski, 2017). The design of the reputation management system is commonly

designed as centralised, which is managed by the website administrator (Resnick et al., 2006). Nevertheless, distributed reputation systems (Kinateder & Rothermel, 2003) have also started to be applied in website design. For example, OpenBazaar an online platform for vendors to sell their products in Bitcoins allows their buyers to send reputation ratings to vendors and the ratings are transparently recorded in Blockchain (Open Bazaar, 2015).

The novel design of our reputation system is that the trust token is not only awarded to the seller and buyer, but also to the decentralised mediator who witnessed the enacted transaction. These reputation tokens are also recorded transparently in the Blockchain as an added advantage to the users to build their credibility.

The Design Stages of Algorithms for Trust in Bitcoin Transaction

The design of the algorithms consists of five main steps briefly described as follows:

Step 1: Pre Transaction between Buyer and Seller
The offline preliminary processes that connect the buyer and seller to communicate, negotiate and have a set of the agreement for the transaction. This includes the agreed Bitcoin price to sell, payment method, trust token fees and the expected completion time for the transactions.

Step 2: Creating a Smart Contract
This step describes the processes to transform the agreement from the previous step into the smart contract to make it valid in Blockchain. By having an agreement in the form of a smart contract, it will support the first suggested design for trust principle, which is a valid contract. The contract is also linked with the multisignature that consists of the buyer and seller.

Step 3: Enacting the Online Transaction with Witness
Once the contract has been validated, a witness will be randomly invited to join the multisignature wallet as a decentralised mediator. Then, the seller will send the Bitcoin to the multisignature wallet. This will make the Bitcoin in the wallet is transparent to the buyer, seller and witness. To release the Bitcoin from the wallet requires at least two signatures. Thus, neither seller nor buyer could release the Bitcoin easily from the wallet without the approval from both of them. This contributes to fair and transparent transactions.

Step 4: Enacting the Offline Transaction
The offline processes involve the transaction of sending the fiat money to the bank account or product through a shipping company. The valid proof of the offline transaction is essential for the transaction's evidence.

Step 5: Sending the Reputation Tokens
Finally, once the offline transaction is accomplished, the buyer and seller may sign to release the Bitcoin from the multisignature wallet. Then the contract will automatically releases the trust tokens to the seller and buyer's wallet as well as wit-

ness token to the witness's wallet. These trust and witness tokens will be associated with their wallet addresses as well as visible on the Blockchain.

6 Conclusion

This research reflects the capabilities of using a Blockchain physical kit, BlocKit to communicate as a design tool to explore the principles and the requirements to design for trust in peer-to-peer bitcoin transactions. Based on the suggestion of the experienced bitcoin blockchain users, a set of algorithms has also been developed to mitigate the trust issue in enacting peer-to-peer bitcoin transactions. Those algorithms can not only be applied for a transaction in between fiat money and bitcoin, but also for the exchanges of bitcoin and products. The highlighted advantage of the algorithm is it maintain the nature of peer-to-peer transaction of bitcoin as created by Satoshi Nakamoto (2008). Furthermore, it also eliminates the transaction fee that normally been charged by the trusted bitcoin exchangers. With the existing of the witnesses for each transaction, it allows not only users to build their reputation in enacting a trusted transaction. Hence this new bitcoin algorithm will be able to elevate the trust for users in enacting transactions without using third party.

References

BTC.com. (2017). Wallet for bitcoin and bitcoin cash. Retrieved April 7, 2019, from https://wallet.btc.com/?_ga=2.71772819.124095.1554668742-553699307.1554668742#/setup/register

BTC Relay. (2016). Frequently asked questions — BTC relay 1.0 documentation. Retrieved April 7, 2019, from https://btc-relay.readthedocs.io/en/latest/frequently-asked-questions.html

Coin Desk. (2019). Bitcoin price index — real-time Bitcoin price charts . Retrieved January 21, 2019, from https://www.coindesk.com/price/Bitcoin

Coin Market Cap. (2019). Cryptocurrency market capitalizations | coinmarketcap. Retrieved January 15, 2019, from https://coinmarketcap.com/

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International Journal of Human-Computer Studies*, *58*(6), 737–758. https://doi.org/10.1016/S1071-5819(03)00041-7

CryptoKitties. (n.d.). Collect and breed digital cats! Retrieved July 19, 2019, from https://www.cryptokitties.co/

Cuen, L. (2018). A decentralizezd bitcoin exchange that's almost decentralized. Retrieved April 7, 2019, from https://www.coindesk.com/Bitcoin-decentralized-exchange-dex-crypto-bisq-dao-monero

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Electrum. (2017). Multisig wallets — electrum 3.1 documentation. Retrieved April 7, 2019, from http://docs.electrum.org/en/latest/multisig.html

Göbel, J., Keeler, P., Krzesinski, A. E., & Taylor, P. G. (2015). Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. Retrieved from http://arxiv.org/abs/1505.05343

Goodhue, D., Lewis, W., & Thompson, R. (2006). PLS, small sample size, and statistical power

in mis research. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (pp. 202b-202b). IEEE. https://doi.org/10.1109/HICSS.2006.381

Horda, T. (2018). What is a smart contract and how it relates to blockchain? Retrieved April 7, 2019, from https://rubygarage.org/blog/guide-to-smart-contracts

Huillet, M. (2018). China's supreme court rules that blockchain can legally authenticate evidence. Retrieved April 7, 2019, from https://cointelegraph.com/news/chinas-supreme-court-rules-that-blockchain-can-legally-authenticate-evidence

Janiszewski, M. (2017). Towards an evaluation model of trust and reputation management systems. *International Journal of Electronics and Telecommunications*, *63*(4), 411–416. https://doi.org/10.1515/eletel-2017-0058

Karamitsos, I., Papadaki, M., Baker, N., & Barghuthi, A. (2018). Design of the blockchain smart contract: A Use Case for Real Estate. *Journal of Information Security*, *9*, 177–190. https://doi.org/10.4236/jis.2018.93013

Khairuddin, I E, Sas, C., Clinch, S., & Davis, N. (2016). Exploring motivations for bitcoin technology usage. In *Proceedings of the Extended Abstracts on Human Factors in Computing Systems ACM* (pp. 2872–2878).

Khairuddin, I. E, & Sas, C. (2019). An exploration of bitcoin mining practices: miners' trust challenges and motivations. In *Proceedings of ACM CHI 2019 Conference on Human Factors in Computing Systems*. Glasgow: ACM. DOI: https://doi.org/10.1145/3290605.3300859

Khairuddin, I. E., Sas, C., and Chris, S. (2019). BlocKit: a physical kit for materializing and designing for blockchain infrastructure. In *Proceeding of the 2019 Designing Interactive System Conference* (DIS '19). ACM New York, NY, USA, DOI: https://doi.org/10.1145/3322276.332237

Khatwani, S. (2018). Best multi-signature bitcoin wallets [2019 Edition]. Retrieved April 5, 2019, from https://coinsutra.com/best-multi-signature-Bitcoin-wallets/

Kinateder, M., & Rothermel, K. (2003). Architecture and algorithms for a distributed reputation system (pp. 1–16). Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-44875-6_1

Leppanen, A. (2010). *Technology Trust Antecedents: Building the Platform for Technology Enabled Performance.* Aalto University.

Lerner, S. D. (2015). RSK white paper overview. Retrieved April 7, 2019,from https://docs.rsk.co/RSK_White_Paper-Overview.pdf

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

Local Bitcoin. (n.d.). How to buy and sell bitcoins online on localbitcoins.com. Retrieved April 7, 2019, from https://localBitcoins.com/guides/how-to-sell-Bitcoins-online

Matzutt, R., Hiller, J., Henze, M., Ziegeldorf, J. H., Müllmann, D., Hohlfeld, O., & Wehrle, K. (2018). A quantitative analysis of the impact of arbitrary Blockchain content on Bitcoin. Retrieved from https://www.semanticscholar.org/paper/A-Quantitative-Analysis-of-the-Impact-of-Arbitrary-Matzutt-Hiller/bb8cef06d139e0959232c471c21f1f7a429b8ddb

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.

MultiChain. (n.d.). Multisignature transactions. Retrieved April 7, 2019, from https://www.multichain.com/developers/multisignature-transactions/

Nakamoto, S. (2008). Bitcoin: a peer-to-peer electronic cash system. Retrieved January 15, 2019, from www.Bitcoin.org

Nielsen, J. (2000). Designing web usability. *New Riders Indianapolis Indiana*.

Omni Layer. (2017). Omni layer. Retrieved April 7, 2019, from https://www.omnilayer.org/

Open Bazaar. (2015). Decentralized reputation in open bazaar. Retrieved April 1, 2019, from https://openbazaar.org/blog/decentralized-reputation-in-openbazaar/

Rahimi, H., & Bakkali, H. EL. (2014). A new trust reputation system for e-commerce applications. *International Journal of Computer Science Issues*. Retrieved from http://arxiv.org/abs/1405.3199

Resnick, P., Zeckhauser, R., Swanson, J., & Lockwood, K. (2006). The value of reputation on eBay: A controlled experiment. *Experimental Economics*, *9*(2), 79–101. https://doi.org/10.1007/s10683-006-4309-2

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human Computer Studies*, *62*(3), 381–422. https://doi.org/10.1016/j.ijhcs.2005.01.001

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

Sas, C., & Khairuddin, I. E. (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* (pp. 338–342). https://doi.org/10.1145/2838739.2838821

Sas, C., & Khairuddin, I. E. (2017). Design for trust: an exploration of the challenges and opportunities of Bitcoin users. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (pp. 6499--6510). Retrieved from http://dl.acm.org/citation.cfm?id=3025886

WeiDex. (n.d.). WeiDex - decetralized exchange. Retrieved April 7, 2019, from https://weidex.market/welcome