An Exploration of Bitcoin Mining Practices:

Miners' Trust Challenges and Motivations

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

Corina Sas
School of Computing and Communications
Lancaster University, UK
c.sas@lancaster.ac.uk

ABSTRACT

Bitcoin blockchain technology is a distributed ledger of nodes authorizing transactions between anonymous parties. Its key actors are miners using computational power to solve mathematical problems for validating transactions. By sharing blockchain's characteristics, mining is a decentralized, transparent and unregulated practice, but we know little about miners' motivations and experiences and how these may impact on different dimensions of trust. This paper reports on interviews with 20 bitcoin miners about their practices and trust challenges. Findings contribute to HCI theories by extending the exploration of blockchain's characteristics relevant to trust with competitiveness underpinning the social organization of mining. We discuss the risks of collaborative mining due to centralization and dishonest administrators, and conclude with design implications highlighting the need for tools monitoring the distribution of rewards in collaborative mining, tools tracking data centers' authorization and reputation, and tools supporting the development of decentralized pools.

CCS CONCEPTS

• Human Centered Computing • Human Computer Interaction (HCI) • Empirical Studies in HCI

KEYWORDS

Blockchain; bitcoin miners; trust; dishonest administrators

1 Introduction

Blockchain technology is a distributed ledger of nodes involved in authorizing bitcoins transactions between anonymous parties [41] whose growth has received increased interest from private sectors and academic communities [3][15][18][28][29][33][48][49]. At the core of blockchain, ecosystems are miners and their validation of transactions through consensus-based proof-of-work. By sharing blockchain's characteristics, mining is a decentralized, transparent and unregulated yet lucrative practice as miners are rewarded in bitcoins for their successfully validated proof-of-work. The reward together with the growing value of bitcoins and their planned scarcity [6][11][41] has attracted more miners to a practice which has become increasingly competitive and computationally taxing [3][38][39].

On the one hand, the purposefully design trustless mining protocol [6][41][46] does not require a third-party entity to authorize transactions but merely miners' consensus, which in turn supports people's trust in blockchain [41][57]. On the other hand, the emerging social organization of mining practices brings forward issues of trust among miners such as the risk of 51% attack [15][19] or of selfish miners [16][25][47][55], explored mostly within the security research area. Relevant HCI works on blockchain and its trust related issues have started to emerge [33][48][49]. We agree with the argument that blockchain offers a unique perspective to explore trust as its characteristics contrast with the centralized, regulated, and non-anonymous traditional transaction systems which have informed the existing HCI models of trust [23][45]. However, apart from modeling-based security research on mining, we know little about miners' practices from their first-person perspective, and how the specific blockchain's characteristics impact on their trust. To address this gap, we report on interviews with 20 Bitcoin blockchain miners about their mining practices and related trust challenges, in order to explore the following research questions:

1. Which are miners' motivations for bitcoin mining?
2. Which are *Bitcoin blockchain's' characteristics* impacting on miners' trust and its dimensions?
3. Which is the *social organization* of mining practices: are there different approaches and types of miners?
4. Which are the main trust *challenges* and how do people attempt to *mitigate* them?

2 Related Work

Our work draws from HCI theories of trust, blockchain technology, and its mining protocol, as well as work in security research on mining-related threats.

2.1 Trust in HCI

In their framework of trust in Bitcoin technology, Sas and Khairuddin [48] identified three trust dimensions: technological (users' trust in Bitcoin technology), social (trust among users, miners, exchanges and merchants), and institutional (government trust in Bitcoin technology). In a later study on bitcoin's users [49], they showed that users' technological trust grounded in the cryptographic protocol is strong, their social trust is challenged by dishonest traders, and that institutional trust should be extended to users' trust in governments and financial institutions. Sas and Khairuddin [49] also showed the feasibility of two HCI theories [23][45] for exploring the trust of bitcoin users. They identified key blockchain's characteristics impacting on bitcoin users' trust such as decentralization, unregulation, transparent, easy, and low-cost transactions.

Corritore and colleagues' model of online trust [23] defines trust as the willingness to be vulnerable and identifies three trust factors: users' perception of technology's credibility, ease of use, and risk. Sas and Khairuddin's [49] findings suggested that for bitcoin users, the blockchain's credibility is supported by the decentralized public ledger, cryptographic protocol, and miners' competence; the ease of use is ensured by ease and quick transactions, while limited risks of institutional abuse of power is supported by the unregulation of blockchain. Bitcoin users' main trust challenge relates to insecure transactions, particularly when dealing with dishonest traders.

Riegelsberger and colleagues' [45] framework on the mechanics of trust explores technology-mediated trust between users, identifying its contextual and intrinsic properties ensuring trust. These include temporal embeddedness of transactions within a past/future timeframe which ensures that parties get to know each other and are motivated to avoid defection in order to sustain future relationship gains. Social embeddedness relates to the earned reputation which parties are motivated to protect; while institutional embeddedness refers to legal aspects which could enforce sanctions when the parties do not meet their contractual agreement. Sas and Khairuddin [49] identified that bitcoin users exploit institutional embeddedness when dealing with exchanges as legally authorized services, and social embeddedness when dealing with reputable traders, underpinned by the temporal embeddedness of repeated transactions.

To conclude, HCI models of trust identified key dimensions of technological and social trust including risks, but their feasibility for the investigation of trust related to blockchain technology has just started to be explored.

2.2 Bitcoins' Blockchain Technology and Mining Protocol

Bitcoins' blockchain technology consists of a distributed ledger hosted by a peer to peer network of full nodes designed by an anonymous entity Nakamoto [34][41][49]. The full nodes' role is to test the validity of each transaction created by bitcoin users, which once approved becomes permanently recorded in the public ledger [34]. The open source mining protocol consists of consensus-based proof-of-work, which is core to the transactions' validation process. Each requested transaction is first verified by the full nodes [7] to ensure that it meets the validity guidelines for inclusion in a new block [7][41], i.e., a record file created every 10 minutes for storing up to 1MB of pending transactions [6][41]. Then, in order to be validated, transactions are broadcasted to the network as part of their block which miners start processing; they compete to be the first to solve the block's complex mathematical problem [6][41]. Once the problem is solved, the miner broadcast their proof-of-work to the network to get the consents from other miners to record the new block in the bitcoin blockchain and the winning miner's block will be verified by the full nodes [7][6][41]. Upon successful verification, the block is recorded on the public ledger, though it is recommended for the merchants, exchanges, and users who accept bitcoin as payment to wait for another 6 new blocks to be confirmed on top of the current block. [6][41]. The winning miner has rewarded 12.5 bitcoins [32]. This number is halved every four years in order to reduce the rewards which demand higher computational power to sustain mining profit. This also reflects the scarcity of bitcoins whose total supply of 21 million will be completed by 2140 [6][35]. Winning miners are also rewarded by transaction fees albeit these are covered not by the blockchain system but by the transaction parties [2][41].

Blockchain's key design features related to mining are decentralization, transparency, and unregulation. In order to ensure its trustworthiness, the mining protocol is decentralized and transparent with all miners having access to the block's problem and the incentive to publicly share their proof-of-work [2][6][41]. The check by consensus facilitates trust in proof-of-work's correctness, ensuring that no single entity can behave dishonestly.

Unregulation, defined as the lack of legal framework underpinning bitcoin mining practices, has been suggested in Nakamoto's vision [41] where blockchain's control is held by miners and users rather than the central governmental or financial institutions. With a few exceptions such as Australia and Germany where the profit from bitcoin mining is taxed, such regulatory frameworks are yet to be developed. While rewards provide a fee-based incentive for miners' competitive search for blocks' solutions [6][37][41], the mining practices also require investment in terms of computational power [12][41] and electricity resources [39].

2.3 Security Research on Mining-related Threats

Most work on mining's trust challenges has taken place in security research area and focused on the risk of an entity owning a large share of the network's computational power. The threat of 51% attack occurs when a group owns over 50% of the computational power of the whole Blockchain network, therefore able to behave dishonestly by performing changes to the protocol or the public ledger's records [15][19]. The other threat is 25% or selfish miners' attack which occurs when miners need at least 25% [25][47], or even 50% of network's computational power [16][41][55].

To conclude, blockchain technology and its mining protocol have been purposefully designed as decentralized, transparent, and unregulated. While these contribute to its trust, they also raise risks and challenges when a mining pool acquires the majority of computational power to control the blockchain. There is however limited empirical work exploring blockchain's features and their impact on miners' trust through qualitative fieldwork.

3 Method

For this study, we recruited 20 miners, with the age range 22-42 (Mean = 30.6). They are all male, with different levels of mining expertise: 8 have over 4 years of mining experience, 8 have between 1 and 4 years, and the remaining 4 have less than one year. Participants have a wide range of professions, including 8 in IT, 1 in the legal services, 2 engineers, 1 in the medical field, 2 teachers, 2 in the financial sector, and 1 in administration. In terms of education, 14 have Bachelor degrees, 4 have Master degrees, and the remaining of 4 are school leavers. The participants are all Malaysian and the recruitment took place via Facebook and Bitcoin Malaysia Telegram group.

Prior work has also focused on Malaysian context for exploring bitcoin-related practices. For example, Sas and Khairuddin [49] argued that it offers a unique opportunity as a developing country with a steady economic growth, increased interest in cryptocurrency [27][36][54], and Fintech regulation [42]. Malaysia has the first blockchain ledger for the public consortium in Asia [14] and aiming by 2025 to fully utilize the technology in the whole country [36].

The recruitment process started by approaching the founder and administrator of the Bitcoin Malaysia group on Facebook, followed by his invitation to the first author to join the Bitcoin Malaysia Telegram group. From within this group, we publicly posted invitations for participating in the study. We also sent private invitations to the most active members of the Telegram group, based on their interest in mining topic as reflected in their contribution to the group's discussion forum.

We conducted semi-structured interviews either face to face or on Skype in both English and Bahasa language from November 2015 to February 2016. The aim of the study was to explore the mining process from the miners' perspective, their motivations and approaches to mining, as well as the main challenges in this process. We also explored participants' risks mitigation strategies. The interviews lasted between 60 and 90 minutes, were audio recorded and fully transcribed. Data analysis followed a hybrid approach with existing concepts being used for the deductive coding while new ones grounded on the empirical data, is used for inductive coding [26]. The deductive coding included concepts from literature on mining protocol such as the mining work process [7][6][41] mining trends [12][21], mining threats [15][16][25][44][47] and concepts from the HCI literature on trust such as technological, social and institutional dimensions of trust [33], temporal, social and institutional embeddedness [23]. The codes were iteratively refined as new codes emerged under the theme of mining approaches, dishonest pool administrators, and risk mitigating strategies.

4 Findings

We begin by describing miners' motivations, the main characteristics of blockchain technology and their impact on miners' trust. In particular, we highlight the social organization and competitiveness of mining practices and how it is reflected on different approaches to mining and types of miners. We further outline the risks of collaborative mining due to centralization and dishonest administrators, and mitigating strategies addressing them.

4.1 Motivations of Bitcoin Miners

In this section, we discussed the three sources of motivation for engaging in mining practice as highlighted by miners.

4.1.1 Earning Potential through Fee-based Rewards. Almost half of participants appreciated the earning potential of mining practice [41] together with the increasing price of bitcoins [11]: *"until today I am still continuously generating profit from this activity; this is my motivation"* [P14]. This steady revenue fosters miners' willingness to continue to invest in such lucrative practice by upgrading the mining equipment. Such capital costs are needed to ensure competitiveness in the context of increasing mining difficulty.

4.1.2 Experimenting with Bitcoin Blockchain Technology. The complexity of the bitcoin mining process is also attractive in itself, as mentioned by 3 participants. For example, from initial curiosity, people developed an interest in both mining and using bitcoins: *"I have the thought like "is this a real thing"? That was the initial direction. Then after mining bitcoins, I transferred mine to the wallet and tried to sell, thinking that if I can get USD for them then this is real"* [P16]. In such cases, participants appreciate the hands-on experience and the knowledge that they gain: *"even though it is considered a high capital investment [practice], mining is good in terms of learning"* [P11].

4.1.3 Lack of Regulation Regarding Taxation of Miners' Fees. Despite its potential to generate income, the taxation regulation of this activity is not yet regulated. As it stands, the discretion to pay tax remains with the individual miners: *"[who may be] willing to pay the tax whenever they get the bitcoins from mining"* [P1]. There is also a concern that in the future the mining practice may become subject to taxation: *"if [governments] decide to monitor mining activities [like] gold or silver then [they] will ask all bitcoin miners to register with the government"* [P2]. This can also have implications with respect to the anonymity of that mining practice.

4.2 Blockchain's Characteristics Impacting on Miners' Trust

Blockchain's key design features related to mining are decentralization, transparency, unregulation, ease of use, and social organization, which has shaped the mining approach and the emergence of different types of miners.

4.2.1 Decentralized and Transparent Mining Protocol. More than a quarter of participants valued the mining protocol both in terms of its complex validation process: "*it uses the cryptographic hashing algorithm to secure the network so you cannot [fake] bitcoins*" [P7], and security: "*I think it is rather difficult at the current computing power for people to hack it*" [P10]. Key to bitcoin's mining protocol is the proof-of-work [41] reflecting miners' systematic and transparent competition for finding the quickest and longest solution to a block: *"this technology is based on the proof of work, where everything is calculated mathematically and is transparent"* [P18]. Participants also expressed appreciation for this cooperative work within the trustless blockchain technology: *"the platform is standard; everyone uses the same blockchain, so I don't think there is a trust issue"* [P2]. These quotes are illustrative of miners' trust in mining technology: competitive, transparent, and decentralized protocol under no control of central entities, which strengthens the credibility dimension of online trust outlined in Corritore and colleagues' model [23].

4.2.2 Non-Legally Binding Practice. No institutional authority such as banks or governments controls blockchain and its mining protocol, which in turn limits the risks of their abuse of power [46]. Although there have been attempts to regulate mining as an arguably lucrative and thus taxable practice [5], in many countries including Malaysia, it is not considered illegal. Four participants expressed satisfaction with the unregulation of mining practice: *"I don't see any issues here: mining is just like you are running a software on a computer"* [P17]. As a result, miners operate anonymously: *"all nodes in the network only know each other pseudo-anonymously and they have the same privilege but yet they can come to the consensus to agree on which record can be written in the database"* [P11]. This unregulation limits miners' perceived risks as a dimension in the model of online trust [23], increasing their trust in mining practice. As shown earlier, there is, however, the awareness that income generated through mining may become subject of taxation

4.2.3 Ease of Use. Participants appreciated the ease of use of the mining protocol and the limited technical skills required. For example, four participants noted their casual experience of bitcoin mining: "*I just let it run and once in a while, I just check to see [...] if it doesn't calculate or the block has been full, or if there is something to do with my wallet which does not allow to receive the bitcoins*" [P2]. Such quotes indicate an important dimension of the online trust [23], ease of use of the mining protocol, which further supports miners' trust in it.

4.3 Social Organization of Mining Practice: Competitiveness

This section explores the complexity characterizing the competitiveness of bitcoin mining practices. It focuses on different forms of mining and types of miners. The identified forms of mining vary across computational power, its ownership, and maintenance which showed increased complexity over time. We grouped these forms in individual and collective mining, taking place on miner's home machines or those leased from data centers (Table 1).

	Individual	**Collective**
Own machines	Home-solo mining *[P2, P5, P12, P18]*	Home-pool mining *[P1, P3, P4, P7, P9, P10, P11, P15, P16, P17 P19, & P20]*
Leased machines	-	Data center-pool mining *Owned: P6; Leased: P8, P13, P14*

Table 1: Mining approaches

4.3.1 Home-Solo Mining. The first form of mining that has historically emerged consisted of individual miners working on their own home machines. A quarter of participants expressed appreciation for this cooperative and competitive work requiring limited computational power [41]. Our findings indicate that 16 participants who mined during 2010-12 have engaged in this form of mining: "*I started as a home miner in 2011, mining on my computer; and at that time bitcoin was not as popular as now*" [P5]. This quote is similar to others confirming the limited mining's difficulty in those early days [6]. With this advantage, home miners worked solely enjoying the full rewards of their labor: "*in early days people use to do solo mining and all profits will straight away go into your wallet*" [P18]. With no intermediaries between the miners and the bitcoin network, the trust consisted solely of trust in the mining protocol, as expressed by three of participants: "*they didn't have any problem to trust each other [...] they mined by themselves and they were referring to the same ledger*" [P3]. This quote reflects the characteristics of trustless blockchain mining protocol which provide a transparent and fair competition among miners for processing transactions [41].

However, at the end of 2010, the mining's difficulty has considerably increased [21]. This, in turn, affected solo miners, due to the small computational power of their individual machines. Two participants shared this view: "*due to high difficulty, solo mining is now no longer relevant*" [P12], and it paved the way for collaborative mining, and in particular for what we call home-pool mining.

4.3.2 Home-Pool Mining. From solo mining, home miners started to shift towards collaborative mining. Mining pools consist of geographically distributed home miners and their network of machines pooling together computational resources and share of the profits [9][6] [10][22] by acting as a sole entity in the competitive solving of blocks' problems. A quarter of participants expressed this view: *"mining pool is actually the entity that controls the hash power in the network [and] the income* *that it generates is divided among miners, according to the hash power that they have contributed to that pool"* [P4]. This indicates that in addition to end miners, a new type of miner has emerged: the pool administrator who creates his own pool to gather the computational power of end miners and automatically divides the mining profits to each miner according to their individual contributed power. As a home pool tend to be small in size [39] usually consisting of 10-15 miners, the equity of profit distribution is not usually an issue. The home-pool mining offers the increased likelihood of success, as reported by two participants: "*I shared with my friend back in the university to buy a second-hand computer and a powerful graphic card. Each of us spent around RM 1500 and we started to mine*" [P19]. Apart from creating such pools, people also started to join existing pools, as mentioned by four participants: *"I mined in a pool because with solo mining it is difficult to get profit"* [P10].

In the late of 2012, after the first halving period [6] the difficulties of mining have further increased [21], negatively affecting home miners, as noted by almost half of participants: *"from normal CPU I upgraded to GPU. The difficulty level was increasing and my system did not generate enough coins. So I stop mining around 2012"* [P5]. This indicates that even though the miners had taken the efforts to improve their machines' computational power, this did not suffice as they faced additional challenges due to higher maintenance costs. For example, four participants noted that in order to continue to mine competitively, the computational power needs upgrading: *"for home mining, let's say you bought the latest S7 mining machine and joined a pool, you can get a few bitcoins for the first few months. [Then] you need to add more hashing power to your machine [because] the difficulty of mining keeps increasing. That's why many home miners retire from doing this job"* [P17]. In addition, maintenance also relates to high electricity cost: *"machine is very expensive and the electricity bill can be around RM100k per month. So you won't get your money back unless you go big scale"* [P3]. Furthermore, three participants pointed to the challenge of locating the machines in their homes due to the generated heat: *"because my house will be very hot"* [P3]. Together, these challenges have led twelve of participants [P1, P3, P4, P5, P7, P9, P10, P11, P15, P16, P17, and P19], to retire from home mining, three [P2, P12, and P18] to continually upgrade their home mining system by creating so-called mining farms, with a cluster of machines owned by one person, and located outside one's home, usually in a rented place. One participant considerably scaled up his mining systems so that "*today I own a data center company for mining*" [P6]. The remaining four participants [P8, P13, P14, and P20] joined directly the cloud mining through data centers.

4.3.3 Data Center-Pool Mining. The increasing challenges of bitcoin home mining have radically transformed it into large-scale mining, beyond the confine of miners' own homes. As noted by three participants: *"as the difficulty of mining is increasing every day, for now, you can only mine at bigger scale"* [P10]. Data centers allow *"cloud mining, where people buy computational power in return for the share of the profit"* [P1]. As pointed out by one participant, data centers also need to mine in pools in order to sustain their profits: *"if you want to mine as an owner of a data center then you need to have large capital [...] at the same time, you have to join a mining pool to make profit"* [P1]. To address these challenges bitcoin data centers have started to emerge [37]: *"the best option is joining the cloud mining, where you can buy a share from the owners of the data center to do the mining for you"* [P9]. Compared to the home mining, data centers require much larger capital and maintenance costs. These include not only the cost of electricity but also of the monitoring equipment and manpower to maintain the center as illustrated in this quote of a data center administrator: *"I used special software monitor [...] I can login from my mobile and I am able to gather data on the current temperature. I also hire a worker to ensure the cabling and network are well maintained"* [P6].

More than a quarter of participants valued the opportunity of data center-pool mining because of the inability to setup their own mining pool: "*the difficulty today is very high and the electricity cost is expensive too. So it is not worth mining at small scale. I think for today, cloud mining is the best way"* [P13]. In addition, leasing the mining service does not require technical expertise: *"data centers offer a 3-year contract, when I get my daily profit from the hired miner [...] When I joined the program, I got the id and password to access to the company website, they also give me a wallet so all profit will be straight away sent to my wallet"* [P20]. Cloud mining is further appreciated because the challenge of machines' maintenance is met by the data center, as highlighted by a quarter of participants: *"for the cloud miners, you don't have the miner at home. It is all maintained in the data center [so] you don't have to pay any utilities. But you have to pay the owner of the data center usually around 20% of the total profit"* [P5]. This and a similar quote: "*I need to pay around 30% of my daily profit for the maintenance fee to the company"* [P9] indicate that the skills of data centers' administrators for setting and maintaining the mining machines comes at a non-trivial cost for the end miners.

4.4 Types of Miners

Findings indicate four main types of miners: end miners, pool administrators, data center administrators, and Bitcoin core developers. These types differ in their expertise, power over the practice, approach to mining and numbers, with the largest number represented by the end miners (Figure 1).

4.4.1 Bitcoin Core Developer. Bitcoin mining protocol is controlled by the five blockchain experts, as mentioned by a quarter of participants: *"bitcoin technology has been created by Satoshi who has passed the responsibility to the Bitcoin core developers. These five persons have the authority to edit the bitcoin code, although any amendments need to meet consensus*" [P5]. Interestingly, almost a quarter of participants expressed concerns regarding the implication of this high power status on the claim of decentralization of the mining practice: *"Bitcoin technology is depending on these five persons which actually contradicts its decentralized principle"* [P1].

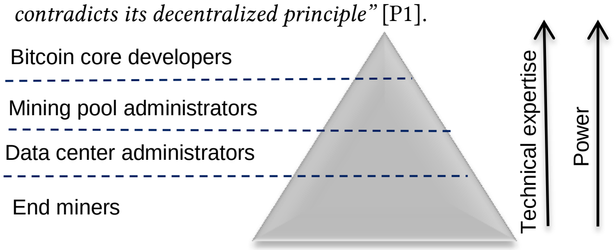

Figure 1: Pyramid of types of miners

4.4.2 Mining Pool Administrator. Pool administrators have emerged within collaborative mining in order to facilitate miners' access to mining pools. Administrators' technical skills are more advanced than end miners' as they are required to set up, run and maintain the machines within the pools: *"currently there are many pools and all miners [...] need to go through those pools which are created by the bitcoin administrators"* [P5], and "*such pools are hard to set up and maintain*" [P12]. Such specialized technical skills are not easy to master and have given administrators the advantage of controlling the mining activity and the distribution of reward. In addition, almost half of participants also acknowledge the high level of skills required by administrators who act as pool manufacturers to develop more competitive mining chips. Mining pools could be joined in by miners with different computational power from end miners owning own machines at home (increasingly unprofitable), to those owning mining farms, or data centers.

*4.4.3 Data Center Administrators***.** The increased mining competition demanded higher computational power. This has made room for data center administrators to enter the scene. They provided end miners the opportunity of leasing machines hosted and maintained within the data centers: "*my friend owns a data center offering cloud mining service"* [P5]. The data centers also join mining pools in order to increase their likelihood of successful mining, but the decision of which pool to join is made solely by the administrator: *"the mining process is controlled by the mining pool"* [P6]. The privilege of pool administrator to distribute rewards to each entity in the pool according to the computational power brought in, cascades down to the data center administrator who further distributes such reward to the end miners within the center.

4.4.4 End Miners. While miners engaged in solo home mining had to develop technical skills for setting and maintaining their own machines, the emergence of collective mining and of administrators supporting it, has led to end miners' deskilling. More than half of participants noted end miners' limited technical expertise: *"it is very easy: I download the software from the pool, I do the setup [...] let my leased machine run for 24/7 [and] I monitor it to make sure that it doesn't crash and is connected to the internet"* [P10].

End miners have limited power, as they are at the discretion of pool administrators for distributing equitable profits. In order to remain competitive, they also have to follow the trend set by their pool administrator for upgrading their leased machines: "*as a miner, we must regularly update our mining machine according to the latest chips produced by the manufacturer, to ensure we are able to maintain the reward"* [P6].

4.5 Trust Challenges of Collaborative Mining

The benefits of collaborative mining are offset by some important trust-related challenges. These pertain to the risks of mining protocol and centralization of mining practices, as well as the challenge of social trust between end miners and data centers/pool administrators.

4.5.1 Risks of Mining Protocol. An important finding is the three challenges of the mining protocol pointed out by most of the participants. These relate to the increased time for acquiring block confirmation, limited block size, and a limited number of full nodes. Interestingly, each of these technology-related risks steams from the purposefully designed blockchain protocol. For instance, multiple confirmations required for recording a block was intended to limit the risk of double spending attack [6][21], but their numbers increased from 3 to 6 leading to delays: *"the 6 confirmations waiting time is bothering me a lot"* [P12], or unconfirmed blocks: *"there were also cases when there was no confirmation for quite sometimes, and the bitcoins were eventually returned back to you"* [P19].

The current blockchain protocol also limits the size of each block to 1MB and about half of the participants expressed concerns: *"this block size limits the transactions acting as a bottleneck"* [P18]. This challenge has received considerable attention in security field [31], and led to increased mining's competitiveness and incentive-based fees: *"people have to increase the mining fee to give a chance to their transactions to be included in the block; however, this removes the benefit of cheap transactions"* [P12]. Not at least, there is a shortage of full nodes designed to host a full copy of the blockchain: "*we have about 6000 full nodes and the number is not sufficient to support the current demand"* [P1].

Although critical for the decentralization of blockchain, the full nodes are resource-demanding [7], and many end miners lack the incentive to host them. Perceived risk in technology is one of the three factors in Corritore and colleagues' model of online trust [[23]. Our findings point to these blockchain design features as risks minimizing end miners' trust in the protocol, especially since they lack both control and high-level expertise needed to address them.

4.5.2 Dishonest End Miners: Selfish Attacks Unconfirmed. A striking finding is our limited empirical evidence of selfish miners' attacks commonly discussed in security research [16][25][47][55]. First, the majority of participants are not aware of such attacks. Second, for the few ones that were aware of selfish miners' attacks, two out of three participants expressed optimism: *"for me, that is just a theoretical concern [because] such attack can only take place only if one has [considerable]* *computational power [which] I would say it is not possible"* [P1]. In addition, another participant extends this argument claiming that even if selfish miners' attacks occur, they can be detected by the protocol: *"yes, this can happen [...] but after a while, the system will know [...] then the system will put the mining server to one side, so then other miners will know that they can't trust that particular mining server at this IP address"* [P7].

Therefore, our findings support the theoretical perspective of Bitcoin core developers [16][55] on the reduced likelihood of such attacks. Indeed, in his original white paper [41], Satoshi mentioned that the bitcoin network is secure, providing the attacking power must not exceed the total collaborative power of the trust nodes. This may be different in the dystopian future suggested by two participants, where the advent of quantum computing may provide sufficient computational power to one pool for a 51% attack: "*current computing power is too high to hack [...] but with the future quantum computer [...] there is a possibility that the bitcoin network will be affected"* [P18].

Although mining is an anonymous practice, the machine IP is visible online, acting as a proxy for its miner. While selfish miners can change their machines, this is unlikely to happen often, which means that the IP offers a history of mining behavior's trustworthiness. This provides support for the temporal and social embeddedness as contextual properties of the framework on mechanics of trust [45].

4.5.3 Centralization of Mining Practices. Findings indicate that mining is a highly competitive practice which requires increased investment in computational power so that miners could continue to generate profit. This trend is consistent with the planned scarcity of bitcoins [21]. Figure 1 shows that the distribution of power among miners is not equal, but concentrated towards the top and middle level of the pyramid.

Centralization is critical with respect to miners' social trust as it entails power imbalance between end miners on the one hand, and mining administrators and core developers on the other hand. It is also aligned with higher technical skills, so that end miners joining pools face the risk of deskilling and of lower profit distributed by the pool administrators.

Centralization of mining occurs both at pool level and between pools, with larger ones contributing with a higher percentage of computational power: *"there is a lot of centralization in a mining pool. Each of the larger pools controls like 20-30% of the contributed hash rate. So miners were actually controlled by the pool that they joined"* [P12].

Findings also indicate centralization by geography, with several participants acknowledging China's massive growth in miners' number [P6] and its dominance of bitcoin mining practices: "*it may have the authority to control the bitcoins price because of its largest bitcoin market share"* [P5]. This dominance is supported by China's low-cost energy supply [56] and effective mining techniques: *"they mine in a very professional way [through] lower and upper cooling systems and proper server racks [using] professional hydroelectric generator and water cooling system to reduce the cost"* [P16]. China also considers legalizing mining practice [52] and is an innovation leader in mining manufacturing: "*capable of designing chips [...] to shrink the size and improve the mining process"* [P3].

These findings challenge the credibility of mining behavior, as a dimension of online trust in Corritore and colleagues' model [23], suggesting that end miners' trust in higher level miners is negatively affected. It also indicates the perceived risk of centralization, with risk being a limiting dimension of trust in the above model [23].

4.5.4 Dishonest Mining Pool and Data Center Administrators. This section further unpacks the challenge of social trust between end miners and data centers/pool administrators. For this, we describe its main sources, steaming from the limited regulatory framework for sanctioning dishonest behavior: lack of audit for the distribution of rewards, the invisibility of data center offering cloud mining, and administrators' lack of accountability.

4.5.5 Lack of Audit for the Distribution of Rewards. The most common trust challenge of dishonest mining pool or data center administrators relates to their privileged position of collecting the computational power of their end miners in order to proportionally distribute the rewards. Unfortunately, some administrators abuse this power, a trust issue mentioned by almost half of participants: *"a trust issue between miners and pool administrators may arise because the administrators are responsible for collecting all the hashing power and distributing the accurate rewards to all miners"* [P3].

This challenge is due to the limited shared knowledge or audit trail of the pool's or data center's overall hash power, which in turn, allows the administrators to report inaccurately smaller profits for their end miners. Indeed, dishonest administrators may claim higher hashes power to attract miners to join in, but report underperformance with respect to the targeted amount of blocks, which in turn allow them to deliver unfairly smaller rewards: *"each [large] pool controls like 20-30% of the hash rate and this amount is not known by the miner"* [P12].

Prior work has confirmed this lack of transparency with respect to the pool's hash power [58]. This outcome extends the value of online information for supporting website credibility [4][40] to mining pools and data centers, particularly the need for information regarding the overall computational power and transparent mechanisms for reward distribution.

4.5.6 Invisibility of Data Centers. An interesting finding relates to the lack of visibility of the cloud computing infrastructure underpinning data centers. Several participants pointed this out: *"I don't have 100% trust in all mining programs that I joined because it is something that I cannot see. I don't even know if the data center really exists"* [P8]. Even if the location of the data center is known, the lack of visibility of the hired machine leads to additional trust challenges: *"I have invested my money, but actually, I don't even see the machine that I bought. It is all kept in the data center, and all I was told is that it is based in*

Iceland" [P20]. This lack of visibility of cloud computing is an important technology-based trust challenge which started to be explored [8][43][44]. Our findings further highlight the importance of online information [4][40] to support trust in data centers, particularly in terms of their physical presence, contactable local representatives, testimonial-based reputation, and authorization from the local administration. Data centers are service providers which arguably should operate within a regulatory framework, and it is surprising that our findings suggest otherwise.

4.5.7 Mining Program Scams: Lack of Accountability. A critical trust challenge relates to deceitful mining programs mentioned by two participants, one of whom has been a scam victim: *"I have joined a mining program [...] at first everything looked fine: I received bitcoins every day for 2 weeks, but then it stopped. I tried to contact the person who introduced me to that mining program but he couldn't be reached and I realized that it was actually a scam"* [P8]. This quite illustrates the concern for leveraging data center's unfunded reputation for attracting end miners, since there are no legal implications of such dishonest behavior. From the perspective of mechanics of trust's framework, these findings shed light into end miners' limited trust on higher level miners because of the lack of institutional embeddedness [45] for legally sanctioning more powerful miners acting dishonestly.

4.6 Mitigating Trust Risks of Collaborative Mining

Findings indicate that end miners employ two strategies for mitigating the risks of social trust in pool or data center administrators. These include selecting reputable major pools, and decentralizing collaborative mining.

4.6.1 Selecting Reputable Major Pools. To address the risk of mining program scams and of unfair distribution of rewards, most miners engage in careful scrutiny of the pool to be joined: "*you must make sure to choose a reputable pool"* [P3]. This is not trivial, as findings indicate that the information provided by the data centers to support such scrutiny is limited which in turn adds to their invisibility challenge.

Unsurprisingly, reputable pools are large and most miners select major pools: *"the main thing is to make sure that the pool is good enough, by looking at the pool contributions and if it is about 30% of the overall, then I think it is good enough"* [P18]. Through their proven history of acting in good faith, reputable major pools offer proxy ways towards reputation, through the motivation to preserve future behavior. This strategy confirms the framework on mechanics of trust [45] on warranting end miners' trust in pool administrators because of their reputation (social embeddedness and credibility), albeit not institutional embeddedness. Prior work has emphasized the importance of accountability in cloud computing to be supported both technically and legally [45]. While reputable pools are perceived as fair, they are not necessarily regulated in terms of being accountable for failing to deliver their contracts with end miners. Indeed, pools do not divulge the identity of their administrators other than by their IP addresses.

4.6.2 Decentralizing Collaborative Mining. A consequence of end miners' preference for reputable large pools is their growth in size, to an extent that such pools could challenge the decentralization principle of mining protocol [6]. A major concern here is that when largest pools are getting close to representing 50% of the network's hash power, they can enable serious negative behaviors such reversing transactions and double spending [16][41][55]. In an attempt to address miners' centralization and circumvent pool administrators, miners have engaged in *"initiatives to build decentralized pool such as the P2Pool"* [P12]. Such pools benefit from the advantage of collaborative mining but without the need of a central administrator [29]. This strategy strengthens the pool's credibility and reputation, reducing the risk of administrators' abuse of power. A limitation of these decentralized pools is that they are challenging to build, currently small with the limited share of the network's computational power and need time to grow [29]. An alternative strategy to address the challenge of centralization of collaborative mining is its self-organization, with miners voluntarily leaving those pools at risk of gaining too much hash power [30]. This strategy strengthens the credibility dimension of online trust depicted in Corritore and colleagues' model [23], as well as the intrinsic properties warranting trust from the framework on mechanics of trust [45] such as benevolence and trustworthiness of end miners and pool administrators.

5 Theoretical Implications

We now discuss the value of our findings for HCI research on trust. Recent work has argued that the exploration of bitcoin-related practices offers unique opportunities to understand trust, as they challenge common assumptions of financial transactions' centralization and regulation [48]. Given the study's focus on a developing country, our implications are mostly relevant for mining in such contexts. They may also hold value for understanding and supporting trust in bitcoin mining practices worldwide, as future work in this emerging research area may focus on exploring.

5.1 Towards a Model of Trust among Bitcoin Miners

Our findings contribute towards a model of trust among bitcoin miners (Figure: 2). They extend previous outcomes on the feasibility of HCI trust theories [23][45][49] and their application not only to bitcoin users [49] but also to miners. We identified blockchain's characteristics impacting on trust. Those supporting trusts include the decentralization, unregulation, and ease of use of the mining protocol, while those impeding trusts consist of specific protocol-related risks, the emerging centralization of the mining practice, and dishonest pool and data center administrators.

According to Sas and Khairuddin's [49] bitcoin trust framework, our findings indicate that the purposefully designed decentralization and unregulation strengthen miners' technological trust. With respect to social trust, outcomes suggest that the main challenge is not among end miners, but between end miners and dishonest pool and data center administrators. In terms of the institutional trust, similar to bitcoin users, miners distrust financial and government institutions, but the unregulation of mining practices mitigates their perceived risk of abuse of power [53]. Interestingly, because of the unregulation, governments' trust in mining practice is lacking behind.

The application of the model of online trust [23] indicates miners' ambivalence towards the technological trust in mining protocol. Findings highlight specific protocol-related characteristics impacting on the three dimensions of trust: credibility, ease of use, and risks. In addition to decentralization, the credibility of the trustless mining protocol is ensured by its transparency, social organization, competitiveness, predictability, reputation, and embedded high-level expertise of the core developers. Miners' trust in the protocol is also supported by its ease of use, but challenged by the risks of increased time for acquiring block confirmation, limited block size, and the number of full nodes.

The framework on mechanics of trust [45] allowed us to explore the social trust among different types of miners and in particular the end miners' risk mitigation strategies for dealing with dishonest pool and data center administrators. Interestingly, although the trust among end miners has not been flagged as salient, the continual use of a mining machine offers through its IP a proxy indicator for miner's reputation (temporal and social embeddedness) [43]. However, given the invisibility of cloud mining, administrators' reputation is more critical and therefore mechanisms for signaling it are much needed.

Additional reasons include the risk of scam due to administrators' lack of accountability and lack of audit for the distribution of mining rewards. To address these risks, end miners' select large pools which have been around for a while and have gathered a large number of end miners. Pools' history offers a proxy for their reputation (social embeddedness and credibility), but their administrators continue to lack the ability to be legally sanctioned for dishonest behavior [45].

5.2 The Paradox of Decentralization

Decentralization is a key principle both of the blockchain and the mining protocol [22][41]. It ensures the distributed network of independent miners engage in competitive-collaborative work for recording the proof-of-work on the block, in the absence of any central authority [22][28]. In contrast to this theoretical principle, findings indicate that in practice there is a strong tendency towards the centralization of mining practices. This is due to its difficulty and growing demand for computational power that miners need to ensure in order to remain competitive.

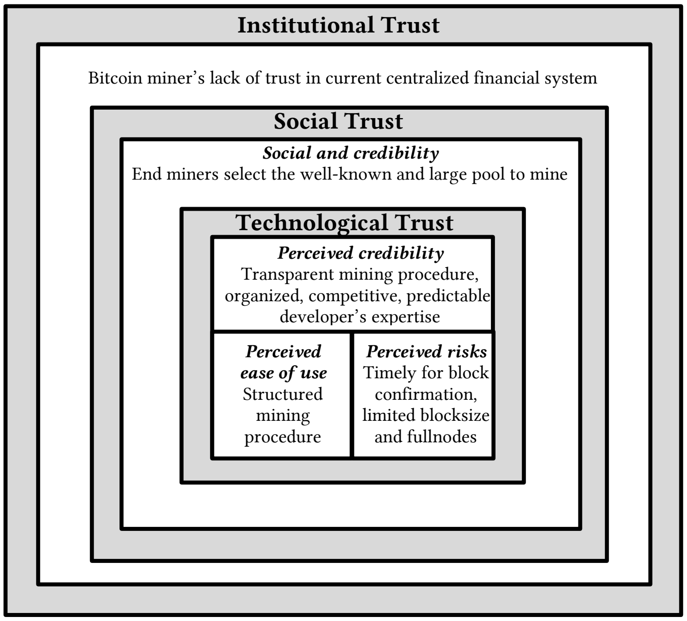
Institutional Trust
Bitcoin miner's lack of trust in current centralized financial system
Social Trust
Social and credibility
End miners select the well-known and large pool to mine
Technological Trust
Perceived credibility
Transparent mining procedure, organized, competitive, predictable developer's expertise
Perceived ease of use
Structured mining procedure
Perceived risks
Timely for block confirmation, limited blocksize and fullnodes

Figure 2: Bitcoin Miner's Trust Model

Currently, the only way to remain competitive is to join one's computational power with that of other miners' in a pool. As an increasing number of miners have joined the most reputable largest pools in the network, we witness the centralization of mining practices within such pools. Our findings indicate that centralization also occurs at a geographic level, particularly because of China's dominance in bitcoin mining and manufacturing. There is also a trend of centralizing miners' power across the different types of miners outlined in Figure 1, with the end miners at the bottom of the pyramid benefitting from the lowest level of technical skills and power to alter the protocol or to distribute the mining rewards. The key strategy to minimize the monopoly of power is by developing fully decentralized pools with no central administrator [29].

5.3 The Challenge of Unregulation

Apart from decentralization, the unregulation of blockchain technology is another key design principle highlighted in Nakamoto's vision [41]. Intended to ensure the privacy of the owners of bitcoin addresses, unregulation also ensures the anonymity of bitcoin miners so that they could continue to support the blockchain irrespectively of its legal status. This, however, raises an interesting challenge when it comes to dishonest miners. Our findings indicate end miners' effort to leverage the limitedly available reputation of pool and data center administrators, i.e., temporal and social embeddedness warranting social trust [45]. They also suggest end miners' inability to legally sanction dishonest administrators, i.e., lack of institutional embeddedness [45].

This is an important finding confirming that in addition to governments [48], the need for regulation has been also expressed by other actors in blockchain ecosystem such as bitcoin users [49], albeit for different rationale, i.e., to sanction dishonest traders. Interestingly, however, data centers are service providers which as business entities are typically deemed to operate within the national regulatory frameworks, particularly if they provide additional cloud-based services subject to taxation. We argue for the value of sharing online information on data centers' authorization. This will strengthen their credibility and reputation which in turn will attract more end miners, while at them time readdresses the current power imbalance between administrators and end miners by empowering the latter with institutional embeddedness [45].

6 Design Implications

We now discuss the design implications [50] that our findings entailed. They highlight the value of new tools for monitoring hash power and reward distribution in data centers and mining pools, decentralized tools for tracking data centers' authorization and reputation, and authoring tools for supporting end miners' development of decentralized pools. These design implications have been developed to address the identified social trust challenge of dishonest administrators, and the risk of centralization of mining practices.

6.1 Tools for Monitoring Hash Power & Reward Distribution

Findings indicate that the most challenging social trust issue of collaborative mining is the unfair distribution of rewards that pool and data center administrators are privileged to perform. This is rooted in a lack of audit of pool's and data centers' computational power. One way to address this challenge is to design monitoring tools to support such an audit and provide transparent mechanisms for the distribution of rewards. Such tools will automatically capture and report key metrics involved in the calculation of profits: overall percentage of pools' or data center's computing power contributed to the network, the number of solved blocks within time unit, the total computing power used to solve each block [17][57] as well as daily total reward, together with the percentage of profit due to each end miner based on their individual power contribution. Mechanisms to implement these have started to emerge for instance in Slush Pool's transparent calculation of hash-proof-rate [51]. This could be extended with open source monitoring dashboards accessible to end miners.

6.2 Decentralized Tools Tracking Data Centers' Authorization and Reputation

Study outcomes also highlight social trust challenges related to the invisibility of cloud mining and lack of accountability of data center administrators. In addition to administrators' willingness to share online information regarding their data center's authorization, their social and institutional embeddedness [45] can be further strengthened. For example, there are already attempts to centralize information on authorized data center offering cloud mining services [1]. We suggest the value of designing decentralized tools for not only capturing data centers' authorization details but also verifying and recording them within the blockchain. Such tools could also include database interface supporting end miners to provide reputation feedback. This, in turn, can help the miners to make informed choices for joining specific data centers.

6.3 Tools for Developing Decentralized Pools

Findings indicate the risk of mining's centralization in larger pools which conflicts with the decentralization principle of blockchain and mining protocol [22][41]. A strategy for addressing this challenge is the development of fully decentralized pools with no central administrator. Although this has been previously suggested, the development of such pools requires technical competency not easily available among end miners [29]. One solution would be new authoring tools supporting and incentivizing end miners to develop decentralized pools. Their design can benefit by drawing from research on the end-user development of open source software and their design tools. This design implication also aligns with prior views, such as Buterin's [17] suggestion for open source cross-platform applications allowing end miners to create mining pools through simple user interfaces.

6 Conclusions

The interview study described in this paper explored blockchain's characteristics fostering and hindering miners' trust, and in particular the risks of collaborative mining and miners' strategies for mitigating them. We further advanced the theory towards a model of blockchain trust by discussing how decentralization, unregulation, ease of use, and social organization impact on both technological and social trust among different types of miners. Findings also led to three design implications that will support blockchain miners develop trust in pool and data center administrators, or circumvent their role altogether.

REFERENCES

[1] Audu Jonathan Adoga, Garba M. Rabiu, Anyesha Amos Audu (2014). Criteria for Choosing an Effective Cloud Storage Provider. In *International Journal of Computational Engineering Research (IJCER).* 4, 2:6-13.

[2] Antonylewis2015 (2015). A Gentle Introduction to Bitcoin Mining. Retrieved https://bitsonblocks.net/2015/09/21/a-gentle-introduction-to-bitcoin-mining/

[3] Alireza Beikverdi and JooSeok Song (2015). Trend of Centralization in Bitcoin's Distributed Network. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing* (SNPD*), 16th IEEE/ACIS International Conference* on 2015, 1-6.

[4] 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.

[5] Ofir Biegel (2016). Is Bitcoin Mining Illegal? https://99bitcoins.com/is-bitcoin-mining-illegal/

[6] Richard Caetano (2015). Learning Bitcoin: Embrace the New World of Finance by Leveraging the Power of Crypto-Currencies Using Bitcoin and the Blockchain. PACKT Publishing, United Kingdom

[7] Bitcoin Core (2017). What is a full node? https://bitcoin.org/en/full-node.

[8] Bitcoin Mining (2017). Bitcoin Cloud Mining. http://bitcoincloudmining.org/en/scam-not-paying/.

[9] Bitcoin.org (2014). First mining pool. http://historyofbitcoin.org/

[10] Bitcoin Wiki (2012). Pool vs Solo.. https://en.bitcoin.it/wiki/Pool_vs._solo_mining

[11] Bitcoins (2017). Bitcoin Price Chart with Historic Event. https://99bitcoins.com/price-chart-history/

[12] Blockchain (2017). Hash Rate. https://blockchain.info/charts/hash-rate?timespan=all

[13] Blockchain (2017). Hash Rate Distribution. https://blockchain.info/pools.

[14] Blockchain Embassy Asia (2016). Introducing the Blockchain Embassy of Asia. http://bce.asia/blog/introducing-blockchain-embassy-asia/

[15] Danny Bradbury (2013). The Problem with Bitcoin. In Computer Fraud and Security. 2013,11: 5-8.

[16] Vitalik Buterin (2013). Selfish Mining: A 25% Attack Against the Bitcoin Network. https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/

[17] Vitalik Buterin (2014) A Next-Generation Smart Contract and Decentralized Application Platform. White paper.

[18] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg and Arvind Narayanan. (2016). On the Instability of Bitcoin Without the Block Reward.. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS '16), New York, 154-167.

[19] Daniel Cawrey (2014). Are 51% Attacks a Real Threat to Bitcoin? http://www.coindesk.com/51-attacks-real-threat-bitcoin/

[20] Eng-TuckCheah and John Fry (2015) Speculative Bubbles in Bitcoin markets? An Empirical Investigation into the Fundamental Value of Bitcoin. In Economics Letters 130: 32-36.

[21] Coin Desk (2017). Bitcoin Difficulty Chart. Retrieved http://www.coindesk.com/data/bitcoin-mining-difficulty-time/

[22] Coin Desk (2014). How Mining Works. Retrieved March 13, 2017. http://www.coindesk.com/information/how-bitcoin-mining-works/

[23] Cynthia L. Corritore, Beverly Kracher and Susan Wiedenbeck (2003). On-line Trust: Concepts, Evolving Themes, A Model. In International Journal of Human-Computer Studies . 58, 6: 738-758.

[24] Florian N. Egger. (2000). "Trust Me, I'm An Online Vendor": Towards a Model of Trust for E-Commerce System Design. In CHI '00 Extended Abstracts on Human Factors in Computing Systems (CHI EA '00), New York, 101-102.

[25] Ittay Eyal and Emin Gün Sirer. (2018). Majority is Not Enough: Bitcoin Mining is Vulnerable. In Communication. ACM 61, 7, 95-102.

[26] 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.

[27] Free Malaysia Today News (2016). Penggunaan Mata Wang Digital Bitcoin Meningkat Mendadak di Malaysia. http://www.freemalaysiatoday.com/category/bahasa/2016/08/01/penggunaan-mata-wang-digital-bitcoin-meningkat-mendadak-di-malaysia/

[28] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf and Srdjan Capkun (2016). On the Security and Performance of Proof of Work Blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security *(*CCS '16).

[29] Arthur Gervais, Ghassan O. Karame, Srdjan Capkun and Vedran Capkun (2014) Is Bitcoin a Decentralized Currency? In *IEEE* Security *&* Privacy.12, 3:54-60.

[30] Nermin Hajdarbegovic (2014). Bitcoin Miners Ditch Ghash.io Pool Over Fears of 51% Attack. https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/

[31] Mike Hearn (2015). On Block Sizes. https://medium.com/@octskyward/on-block-sizes-e047bc9f830

[32] Karim Jabbar and Pernille Bjorn (2017). Growing the Blockchain Information Infrastructure. In CHI '17. Proceedings of Conference on Human Factors in Computing Systems, Denver, CO, USA, 6 - 11 May 2017. New York, NY, USA: ACM Press, pp. 6487–6498

[33] Irni Eliana Khairuddin and Corina Sas (2016). Exploring Motivations for Bitcoin Technology Usage. In Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems, (CHI'16) 2872-2878.

[34] Yong Ming Kow and Xianghua Ding (2016).“Hey, I Know What This Is!”: Cultural Affinities and Early-Stage Appropriation of the Emerging Bitcoin Technology. In GROUP '16. Proceedings of the ACM International Conference on Supporting Group Work, Sanibel Island, FL, USA, 13 - 16 Novemenber 2016. New York, NY, USA: ACM Press, pp. 213-221.

[35] Caitlin Lustig, and Bonnie Nardi (2015). Algorithmic Authority: The Case of Bitcoin. In HICSS '15. Proceedings of the Annual Hawaii International Conference on System Sciences, Kauai, HI, USA, 5 January - 8 January 2015. Washington, D.C., USA: IEEE,. pp. 743–752

[36] Malaysia Industry-Government Group for High Technology. 2017. Malaysia Sasar Guna Blockchain Tahun 2025. http://www.might.org.my/blog/2017/02/24/malaysia-sasar-2025-guna-blockchain/

[37] Bill Maurer, Taylor C. Nelms and Lana Swartz b (2013). “When perhaps the real problem is money itself!”: the practical materiality of Bitcoin. In Social Semiotics. 123: 261-277.

[38] Rich Miller (2014). As bitcoin infrastructure booms, mining heads to the data center .http://www.datacenterknowledge.com/archives/2014/01/21/bitcoin-infrastructure-mining-data-center/

[39] Jerome Morrow /(2014). The History of Bitcoin Mining. https://blog.cex.io/cryptonews/evolution-of-bitcoin-mining-12312

[40] Fiona Fui-Hoon Nah and Sid Davis (2002). HCI Research Issues in E-commerce. Journal of Electronic Commerce Research 3.3: 98-113.

[41] Satoshi Nakamoto (2008). Bitcoin: Peer to Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[42] Fintan Ng (2016). BNM Governer Says Fintech Regulatory Ready by 2017. http://www.thestar.com.my/business/business-news/2016/05/26/bnm-governor-says-fintech-regulatory-framework-ready-by-july/

[43] Siani Pearson and Azzedine Benameur (2010). Privacy, Security and Trust Issues Arising from Cloud Computing. In Proc., IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom). 693-702.

[44] Jamie Redman (2016). Hash Ocean: Another Cloud Mining Scam? https://news.bitcoin.com/hashocean-cloud-mining-scam/

[45] Jens Riegelsberger, M. Angela Sase, and John D. McCarthy (2005). The Mechanics of Trust: A Framework for Research and Design. In International of Human-Computer Studies. 62, 3: 381-422.

[46] Arthur J, Rolnick and Warren E. Weber, W (1997). Money, Inflation and Output Under Fiat and Commodity System. Journal of Political Economy. 105, 1308-1321.

[47] Ayelet Sapirshtein, Yonatan Sompolinsky and Aviv Zohar (2015). Optimal Selfish Mining Strategies in Bitcoin. https://arxiv.org/abs/1507.06183

[48] Corina Sas and Irni Eliana Khairuddin (2015). Exploring Trust in Bitcoin Technology: A Framework of HCI Research. In Proceedings of the Annual Meeting of the Australian Special Interest Group for Computer Human Interaction (OzCHI '15), 338 - 342.

[49] Corina Sas and Irni Eliana Khairuddin (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. (CHI’ 17), 6499-6510.

[50] 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) 1971-1980.

[51] Slush Pool (2017). Hash Proof Rate.. https://slushpool.com/stats/hashrate_proof/

[52] Evander Smart (2015). Top 10 countries in which bitcoin is banned. https://www.cryptocoinsnews.com/top-10-countries-bitcoin-banned/

[53] Ramesh Subramanian and Theo Chino (2015). The State of Cryptocurrencies, Their Issues and Policy Interactions. Journal of International Technology and Information Management. 24,3:2.

[54] The Edge Malaysia Weekly (2015). How Have They Performed? https://www.fxinter.net/en/free-realtime-forex-news.aspx?ID=139909&direct=How+have+they+performed%3F+(Part+1)

[55] Kyle Torpey (2015). What is Selfish Mining and is it a Threat to bitcoin? http://coinjournal.net/what-is-selfish-mining-and-is-it-a-threat-to-bitcoin/

[56] Lindsay Wilson (2013). The Average Price of Electricity, Country by Country. Retrieved March 29, 2017. http://www.theenergycollective.com/lindsay-wilson/279126/average-electricity-prices-around-world-kwh

[57] Aaron Van Widtum (2016). A primer on Bitcoin Governance, or Why Developers Aren’t in Charge of the Protocol. https://bitcoinmagazine.com/articles/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427/

[58] Aaron Van Widrum. (2016). Slush Pool Introduce Provably Fair Bitcoin Mining https://bitcoinmagazine.com/articles/slush-pool-introduces-provably-fair-bitcoin-mining-1455217308/