# Of Two Minds, Multiple Addresses, and One Ledger: Characterizing Opinions, Knowledge, and Perceptions of Bitcoin Across Users and Non-Users

**Xianyi Gao, Gradeigh D. Clark, Janne Lindqvist**
**Rutgers University**

## ABSTRACT

Digital currencies represent a new method for exchange – a payment method with no physical form, made real by the Internet. This new type of currency was created to ease online transactions and to provide greater convenience in making payments. However, a critical component of a monetary system is the people who use it. Acknowledging this, we present results of our interview study (N=20) with two groups of participants (users and non-users) about how they perceive the most popular digital currency, Bitcoin. Our results reveal: non-users mistakenly believe they are incapable of using Bitcoin, users are not well-versed in how the protocol functions, they have misconceptions about the privacy of transactions, and that Bitcoin satisfies properties of ideal payment systems as defined by our participants. Our results illustrate Bitcoin's tradeoffs, its uses, and barriers to entry.

### Author Keywords

Bitcoin; digital currency; crypto-currency; interview study

### ACM Classification Keywords

K.4.4 Electronic Commerce: Cybercash, digital cash; H.5.m. Information Interfaces and Presentation (e.g. HCI): Miscellaneous

## INTRODUCTION

For the longest time, money has had associated physical representations; a token has always been required to access and use it. Fiat money is typically minted on coins and paper notes whereas electronic money has credit and debit cards. A 2014 survey indicated a major change in the way US people would prefer to manage their finances: only 9% of participants preferred to use cash and 2% preferred checks [30]. The main cause is the advent of payment methods that offer a superior user experience, such as electronic cards. The newest way of managing payments in an interconnected, mobile world is by using digital currencies (or cryptographic currencies). Personal finance and digital currencies together have been of research interest to the CHI community [32, 33, 36, 57, 39, 45, 55, 14].

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than the author(s) must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
*CHI'16*, May 07–12, 2016, San Jose, CA, USA
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-3362-7/16/05...$15.00
DOI: http://dx.doi.org/10.1145/2858036.2858049

Using the Internet to instantiate a virtual representation of money without a physical counterpart is not a new concept. Electronic cash has existed since Chaum proposed e-cash [13] in 1983, but it failed to take hold since it required banks to adopt it and back up the money with physical notes. The first successful version of digital currency is therefore one that removed the middleman (e.g. banks): Bitcoin. Bitcoin [44] is a decentralized digital currency proposed in 2008 that relies on the collective work of a distributed peer-to-peer network to maintain a public ledger of account history for all of its participants and to verify transactions amongst different actors.

Bitcoin is interesting as a digital currency as it represents a new type of money that solely depends on the decentralized peer-to-peer network to make the transactions happen between two people with degrees of anonymity, across continents, at any denomination, and without any transaction fees going to a third-party institution. A recent article in the Interactions magazine argued why both everyday consumers and designers should care about Bitcoin [14]. The article pointed out that a decentralized transaction management structure and the content storage system inherent to Bitcoin's architecture may have the potential to change the way we think about all transactions and exchanges in the future. With the additional advantage, Bitcoin's underlying architecture can also be widely applied to domains other than finance.

Bitcoin has experienced exponential growth in: the amount of currency mined (14.5 million coins [7]), capital invested (market capitalization of 3.3 billion dollars with a current price of $227 per bitcoin [16]), community involvement (4.1 million people [6]), and a collective computing power base that exceeds that of modern supercomputers. Bitcoin has been the recent darling of technology and security researchers [9] – but money is very much a psychological and societal construct, and it is worth discussing with users what their perceptions and knowledge of Bitcoin are to better understand the context under which it exists. In addition, the number of Bitcoin adopters is still low compared to long-standing fiat currencies. Understanding why more people have yet to adopt this burgeoning currency given its potential for easing transactions can lead to advances in how people manage their finances as well as inform Bitcoin developers how to further improve the user experience.

Different actors have different motivations, knowledge, and experience with Bitcoin. In this paper, we conducted semi-structured interviews with ten users and ten non-users to investigate their opinions and understanding of Bitcoin. For both users and non-users, we gauged their level of understanding on defining what Bitcoin is and explaining how it

operates. We probed our user participants more deeply with questions regarding technical components and their user experience. In addition, we asked our participants questions regarding privacy and security, investment activity, regulatory opinions, and about other payment systems.

Based on responses from user and non-user participants, this paper presents the following contributions: (1) Non-user participants often claim that they cannot use Bitcoin because of a lack of technical knowledge. This is unnecessary for performing transactions. (2) Our interview results reflected that people who actively use Bitcoin are not well-versed in its mechanics. (3) Bitcoin users had misconceptions about Bitcoin's ability to preserve the anonymity of its consumers. (4) User participants advocated for government insurance of Bitcoin deposits despite being largely anti-government and anti-regulation. (5) There is a mapping between participant perceptions of what constitutes an ideal payment system and aspects of Bitcoin across both interview groups.

**Notes:** We use "Bitcoin" to refer to the system and "bitcoin" to refer to the unit of account in the system [9]. Also, we refer to participants recruited from Bitcoin communities as "user participants" (or "users") and those outside of Bitcoin communities as "non-user participants" (or "non-users").

## BITCOIN FUNDAMENTALS

In this section, we give a high-level description of the Bitcoin protocol. Any term that is bolded is a specific technical term that is part of common Bitcoin parlance.

Bitcoin is a peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through any financial institution [44]. Digital currencies have previously been plagued by the **double spending problem**, which means spending the same unit of money more than once. Electronic representations of money that are directly analogous to physical currency dictate that the money must be represented as data on a drive; however, this data can be copied when transferring the ownership. Bitcoin solves this problem by having the majority of participants agree on a global, public ledger of accounts that contains all movements of money between people since the system's inception – this ledger is referred to as the **blockchain**. Agreeing on a global, public history is not enough – a large set of dishonest people could agree on incorrect histories to control the system. Bitcoin prevents this from happening by requiring people to solve a computational problem in order to write to the blockchain. Solving the computational problem involves assembling a **block**. A brief structure of blocks and the blockchain is shown in Figure 1. The blockchain is so-named because what is written to the ledger are these blocks; the history is one long daisy-chain of them.

When someone wants to transfer money, the person broadcasts a message to the network stating the intention – this message is called a **transaction**. The simplest representation of a transaction consists of three components: an amount of bitcoins to send, an **address** representing a person to whom bitcoins are being sent, and a private key used to sign and verify the transaction. The **address** is a public key owned

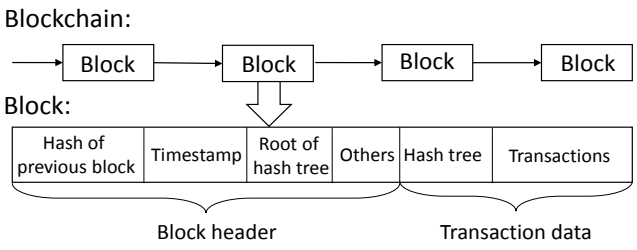


**Figure 1. Bitcoin blockchain structure: The blockchain consists of a long list of Bitcoin blocks. Each block includes a block header and transaction data. The hash tree stores hashes of transaction data.**

by the recipient. Addresses are generally used only once in Bitcoin, and as such users will keep a collection of keys for redeeming bitcoins at those addresses in a **wallet**. There are some online Bitcoin sites (e.g. Coinbase, BitPay, Bitstamp) that help manage Bitcoin wallets and facilitate conversions to fiat currencies.

The people who try to assemble the blocks are called **miners** and the process of solving the computational problem for each block is called **mining**. Mining is computationally wasteful as miners incur losses in the form of electricity, heating, and bandwidth. As such, miners are rewarded with a number of bitcoins mined to incentivize them to verify and post transactions. This means that mining has the dual purpose of introducing new bitcoins into circulation. The total supply of bitcoins is designed to be kept constant at 21 million. The system is tuned, based on the performance of the miners, to create six blocks per hour.

To moderate the network from mining all 21 million bitcoins too rapidly, the number of awarded bitcoins per block halves after certain block goalposts are met. As of this writing, the block reward is 25 bitcoins; the reward will fall to 12.50 bitcoins once 367,500 blocks have been mined [5].

Bitcoin claims to have near-zero transaction fees since there is no centralized third party (e.g. a bank) imposing fees for moving money between accounts. Furthermore, privacy is meant to be given to all participants through removing all identifying markers and just representing users by transactions and addresses on the public ledger. However, transaction fees do exist in this structure – people can pay a premium to have their transactions verified more quickly by aggressive miners.

## RELATED WORK

In this section, we discuss both background and related work on Bitcoin, and prior studies on payment systems.

### Bitcoin

There has been myriad work examining the economics of Bitcoin. Although intangible, Bitcoin has economic value: it remedies the double spending problem, has low transaction fees, and detects fraud through public authentications [52]. The price formation model of Bitcoin appears to follow standard supply-and-demand, though demand is the larger determinant given the supply is limited [15]. Bitcoin's market impact model appears to fit well with statistical latent

order-book models [21]. It remains unclear if consumers will treat Bitcoin as a currency replacement or as a commodity for speculation in the long-term [19]. Other work has analyzed: Bitcoin's money flow and wealth accumulation [34], using Bitcoin as a measurement of socio-economic signals [26], Bitcoin's economic limitations as a decentralized currency [27, 23], and predicting the end-of-day close-price with social media chatter [31].

Previous studies have shown issues regarding security and anonymity of the Bitcoin system. It is claimed that the large computing power needed to control the public ledger is the chief deterrent towards collusion, dishonest mining strategies, and other attacks. This assertion has since been challenged, and it has been demonstrated that a colluding pool with a minority share of the computing power can manipulate the system [24]. The Bitcoin system purportedly preserves anonymity by only identifying users by transactions between addresses that hold bitcoins without any other personal information [29]. However, it has been shown that wallet addresses can be combined with publicly scrapable metadata from Bitcoin discussion sites to identify users [48].

Few studies so far have explored Bitcoin usability and its users. A study in 2013 investigated the social semiotics of Bitcoin and provided an anthropological perspective on Bitcoin users [40]. The work contributed to debate of the privacy, labor of Bitcoin miners, and value of Bitcoin. An indirect approach, by analyzing Google Trends data, has recently been applied to examine characteristics of Bitcoin users and to deduce motivations driving interests in Bitcoin [58]. The work showed that computer programming and illegal activity terms are positively correlated with Bitcoin interest, while e.g. libertarian and investment terms are not. To further investigate the culture of Bitcoin users, a recent study found that users preferred algorithmic authority to the authority of conventional institutions which they saw as untrustworthy [38]. Meanwhile, Bitcoin usability studies indicated that most stakeholders considered perceived ease of use for Bitcoin still rather low [3]. More work is still needed with the usability of Bitcoin key management although it has introduced new ideas compared to older systems [22]. A comprehensive survey and analysis of current academic research into Bitcoin resulted in an outline for future threads of research [9] and revealed the need for more studies on motivations and attitudes of the Bitcoin population.

### Payment Studies

Other studies have focused on how members of different populations use payment systems. Populations of advanced age (eighty years or older) have shown that people mistrust newer or unknown methods of payments [56] (online banking is the case in this study). In one way to address this lack of trust, aging populations were presented with a system called Cheque Mates [55], wherein a digital pen would transfer handwritten checks onto a computer to be verified via crowdsourcing.

General lessons on digital currencies can be gleaned from studying cultures with an abundant amount of these currencies. Based on a study of Japan, which has many digital forms of money [39], digital money should: reduce commotion, be centered around public use, support money management without increasing burden or degrading user experience, engage multiple senses, and be fun to use [39]. In addition, studies about local currencies and crypto-currencies suggested that a currency should also enhance social connectivity and encourage collaborative creation of value through payments and exchanges [11, 25].

Studies have shown that emotional and historical experiences play just as important a role as economic self-interest when people make financial decisions [33]. Finally, there have been studies about monetary transactions through the lens of social context: how money is used in poorer areas [17], how people make decisions to allocate their funds [59], how marriage affects financial status [49], how the elderly perform modern banking [54], and how to optimize user interfaces for newly adopted mobile payment schemes [41].

In contrast to previous work, this paper contributes an analysis of the knowledge and opinions that affect the way people perceive Bitcoin. We focus on discussions with people about how they are currently using this digital currency, how well they understand it, and how they compare it to common payment methods today. Moreover, we contrast this by discussing Bitcoin with outsiders to try to identify how the media or their social network has framed their perception of the currency and what it might take for them to consider using it. Together, the two groups form a picture of the current context under which Bitcoin exists today.

## METHOD

In this section, we describe our recruitment process, the demographics of our participants, our interview procedure, and the interview coding.

### Participants

We recruited 20 participants aged 18 years or older across the United States, of which 10 were Bitcoin users and 10 were non-users. Bitcoin users were recruited online from Bitcointalk [4] and Reddit [46] and non-users were recruited on our university campus via flyers and online using Craigslist [18]. We created two different sets of recruiting material for our two groups: (i) our recruitment material for Bitcoin users explicitly stated our interest in interviewing people who actively used Bitcoin, and (ii) our recruitment material for non-user participants stated that we were conducting a study on currency and payment systems and were interested in interviewing people to discuss these topics.

We refer to our recruited Bitcoin users as U1 to U10 and non-users as N1 to N10. Majority of our participants were of age ranging from 21 to 44, expect one non-user who was 62 years old. Our ten Bitcoin users were all male; this is likely due to the Bitcoin community being 95% male [47, 8]. The ten non-users included four females and six males. Our users' educational background varied from high school to college; our non-users' background varied from high school to graduate school. Both users and non-users had various occupations (e.g. engineers, managers, counselors, business owners).

### Interview Procedure

Our participants were spread across the United States. Therefore, we opted to conduct semi-structured interviews in person, by phone, and through Skype during July 2014. Two authors of this paper were conducting the interviews. The interview process and the list of questions were pre-written in a script to ensure consistency across different participants. The interview questions focused on a participant's preference concerning payment methods, their knowledge and opinions on digital currencies, awareness of Bitcoin, and any experience with Bitcoin transactions. When necessary, we also asked follow-up questions to clarify the participants' responses. Each interview lasted for roughly 30 minutes. Later the audio recordings were transcribed to text for interview coding. Each participant was compensated with a $10 VISA gift card for completing the study.

### Interview Coding

Two authors participated in the interview coding. Applying procedures suggested for constructing grounded theory [12], we started with open coding to generate labels from interview responses and several themes emerged from participants' views on each topic. Then, we used axial coding for further categorization and found several concepts and themes. Ambiguous scenarios during the coding were discussed among our group. Coding was proofread and re-coding was done several times for some topics to ensure reliability of our results. Representative samples of participants' quotes will be shown as we present the themes in the findings section.

## FINDINGS

In this section, we present the findings that emerged from our semi-structured interviews with our 20 participants.

### Bitcoin Background

We asked all of our participants, if they asserted that they knew what a bitcoin is, to define the term and explain briefly how the protocol works. Half of our user participants answered using generalities; one participant explained in detail.

The responses of five user participants reflected a partial understanding about Bitcoin: U1 and U6 both defined Bitcoin as an Internet currency that is scarce, impossible to counterfeit, and has economic functionality similar to that of gold, with U1 saying: *"Gold is scarce, and Bitcoin is also scarce, but if you wanted to pay a dollar in gold, you'd have to break up a piece of gold bar and hand it to someone. With Bitcoin, if you want to send me a dollar's worth of Bitcoin, it'd be as easy as sending an email."*; U5 framed his response in a circular way, saying: *"Bitcoin is an address. ... It's an address that holds a certain amount of units of bitcoins."*; U7 and U10 explained what they knew from using bitcoins, mentioning that a key is needed (U7) and transactions can go globally (U10).

Only one of our ten user participants phrased their response in a way that demonstrated deeper understanding. U9's explanation said that, first, an account would be needed from Bitcoin network to generate transactions for miners to verify. He explained the chain-of-custody: *"you can also verify that the person created a bitcoin according to the Bitcoin protocol. And therefore there's this consensus that this Bitcoin is legitimate. ... And now you, the holder of this private key on this Bitcoin, can then spend it and use it to make transactions on the Bitcoin network."*

The remaining four users had misconceptions: U2 and U8 misrepresented how a bitcoin is defined, with U2 saying: *"I think it could be regarded as just something that sits like a piece of code in basically an electronic form. And it's considered to have a value which makes it a currency."*; U3 and U4 both mentioned that a bitcoin is the reward for solving a mathematical problem, with U3 saying: *"To the best of my knowledge, a bitcoin is a mathematical problem that has been solved by computer and the bitcoin was the reward for solving the equation."*. In contrast, a bitcoin is just an account on the public ledger while the purpose of the protocol is not about solving mathematical problems for rewards – that exists only to incentivize transaction verification.

Six non-user participants asserted that they had at least heard about Bitcoin; the remaining four responded in the negative. N2 believed it was a currency used expressly for black market purchases: *"I've heard of it. It is part [of] currency used for black market sales."*; N3 knew of bitcoins through the context of a financial instrument, saying: *"It's a new currency, basically. To me it seems very speculative."*; N4 was aware that Bitcoin was growing in popularity, but did not know what it is; N9 and N7 referred to Bitcoin as a virtual currency, with N7 believing that it is *"technically complicated and difficult to use in practice"* without explaining why; N8 demonstrated the deepest awareness, stating: *"It's a purely electronic currency. An individual bitcoin is some ridiculously long number arrived through a particular algorithm. I know people who do mining and have their machines spending all extra cycles computing out these algorithms."*

### Bitcoin Usage

Several themes emerged about how participants used Bitcoin.

**Patterns of Use:** We probed our user participants about how frequently they made transactions. Five of our participants (U1, U4, U6, U8, U9) did it heavily, two (U3, U7) used it occasionally, and three (U5, U2, U10) rarely used it. We define heavy use as daily, occasional use as at least twice a month, and infrequent as six months or longer.

We asked the ten non-user participants if they had ever considered using Bitcoin. Eight of them said they did not know enough about Bitcoin to comfortably use it: four of these eight non-users had not heard about Bitcoin; the other four (N2, N3, N7, N9) heard about Bitcoin and they stated they did not enough about how it works to use it. For example, N3 said, *"Never used it. [I] first learned about it in the news, reading an article. ... I don't know how it works technically. There's a whole algorithm behind it."* Similarly, N9 stated, *"Lack of knowledge about them [bitcoins]. ... It's computationally complicated from what I know. It's suspicious."*

The remaining two non-users either did not feel the need to use them or were misinformed about how they could be used – for example, N4 said: *"I didn't need to pay with that [bitcoins]. I could pay with what I have now."*; N8 thought bitcoins could only be obtained from mining, stating: *"Well, I*

*don't have any bitcoins and I haven't really had any computers that are powerful enough to really do any effective bitcoin mining... I'm not sure who actually accepts bitcoins as payment."* In fact, one can easily purchase them through Bitcoin exchange websites (e.g. bitstamp, coinbase) unless the individual prefers mining new bitcoins. None of our non-users have attempted to use bitcoins.

**Bitcoin: Investment or Currency?** The Bitcoin community is split between people who speculate and those who believe in its long term potential. Five of our participants (U1, U3, U4, U5, U8) treated Bitcoin as both an investment and a currency, with U5 opining: *"It's like an investment in the way that you can see the price rise over time. You can hold it, sell it. Just like any other investment ... As a currency, it's accepted at Overstock and Amazon [e.g. bitcoins can be directly redeemed to Amazon gift cards], and you can use it as a way to acquire goods."*; U2, U10, and N4 said Bitcoin was more like an investment – U10 observed, *"I think at this point it's more of an investment. The value is far too volatile to be buying it and holding it as a currency.* U6, U7, U9, and N3 thought Bitcoin was more like a currency, U7 commented: *"It's a currency although it's got a long way to go before it can be a useful high volume thing. Right now there are a lot of technical aspects, the most basic of which is block size limit."*

When asked about whether bitcoins have value as an investment, eight of the ten users indicated reasons that they believed so: personal experience (U1, U3), the upward trend of the price (U5), expectation and confidence (U6, U8), long-term popularity (U9, U10), and smart people (e.g. developers) behind controlling the price (U4). Two users thought of investing in bitcoins as a risky venture, with U2 saying:*"Definitely a risky one because it's still like a new concept. It can either flop or it can go up depending on how much people want to use it."* Only one non-user participant (N4) provided thoughts about investment potential, commenting that bitcoins appeared as a good investment to her because acquaintances had profited from investing in them.

### Security and Privacy Issues

All user participants responded in the affirmative when queried about whether Bitcoin is secure, with U3 declaring: *"If done properly, I would say so, because of the confirmation aspects of it..."* When comparing to bank security, U3 continued: *"Bitcoin is better protected, because I have my bitcoins offline so unless someone finds where they are hidden, I do not think that they could be taken from me."*; U9 also thought that a Bitcoin wallet is more secure than a bank, saying: *"In defense of a Bitcoin wallet, you control yourself. You have access over your private keys. This for sure is more private and secure than other sorts of financial transactions. ... [For banks,] you're trusting a third-party with your money and your activities."* U1, U7, and U9 also compared Bitcoin with other traditional payment methods. U9 continued and mentioned that Bitcoin addresses have stronger encryption methods than credit card payments, with almost no ways to hack it if properly handled. Similarly, U7 thought bitcoins were more secure than using credit cards, stating: *"The credit card is insecure. People can see the numbers. Because of the cryptography in bitcoin, [it is] very secure. It's more secure than many things."* Other participants responded that bitcoins are only protected as long as account information is properly managed – for example, U4, U5, U8, and U10 said Bitcoin should be secure as long as users exercised caution with their keys, with U5 reasoning: *"Due to high computational power involved, they [attackers] cannot counterfeit them [bitcoins]."*

We then asked our participants about whether privacy is preserved in the network. Most Bitcoin users (nine out of ten) thought there is good privacy protection, with U7 comparing it to credit cards: *"The credit card by definition is inprivate [not private]. You're giving away private information to someone in hopes that they don't use it again. Bitcoin security is on a person-to-person level. In my hands its much more secure and private."* U3, U4, U6, and U9 said Bitcoin is almost anonymous. U3 said, *"You can be almost anonymous if you choose to do it that way. It's safe, it's easy to travel with."* U9 also added: *"... the fact that there are privacy implications, that can be important. Not so much for a regular person, perhaps, but there are people really value their privacy for one reason or another and Bitcoin makes it possible."* On the other hand, U1 believed that Vericoin (another cryptocurrency [53]) had better privacy protection, saying: *"it has anonymity capabilities built in, which is better than Bitcoin."* All non-user participants declined to answer the question.

### Technical Aspects of Bitcoin

We also probed our user participants about the fine-grained details of the Bitcoin protocol. We did not ask any of these questions to our non-user participants.

**Bitcoin mining:** The majority of our users (besides U5, U7, U8) had not participated in any mining, with main reasons being high hardware requirements and lack of benefit. They had varying degrees of mining knowledge: half of them gave accurate responses, one demonstrated a high-level understanding, and one did not know about it.

Responses from U1, U2, U6, U7, and U9 were all correct, pointing out that the goal of Bitcoin mining is to maintain, update, and verify the transactions. For example, U1 said, *"Bitcoin mining is the act of maintaining and updating the transaction ledger for the currency and in the cost of doing that, they are receiving a share of the new coins that are being mined, as well as transaction fees."*

U9 gave a more detailed description about mining: *"Bitcoin mining is the process of building the blockchain which is the ledger of all of the transactions that happen on the Bitcoin network... Miners take all the valid transactions they want to include [in the block], ... hash that data with SHA2 [algorithm] ... They create a chunk of data with valid Bitcoin transactions. ... publish or broadcast this block. ... All other miners can verify that all the transactions included in it are valid ... and the miner who found this block gets awarded. ... So, basically, there's no party that can control the transactions going to the Bitcoin blockchain unless they hack into long-term control of over 50% of the hashing power. ..."*

Others were unsure about the intricacies behind the mining process (including U5 and U8 who tried mining previously), briefly mentioning mining as "an important transaction process" (U8, U10), "solving mathematical problems" (U3, U4), and "finding new addresses for a bitcoin" (U5).

**Transactions:** We then asked participants to define transactions in terms of the Bitcoin parlance and to explain the verification process. U1 provided a brief explanation, saying *"a Bitcoin transaction is just an entry in the ledger, moving bitcoins from one account to another."*; U4 and U5 stated that the Bitcoin network *"verified transactions and ensured no double spending."*; U6 and U8 simply said transactions are the action of bitcoins moving from *"one Bitcoin wallet to another."*

Participant U9 again provided the most comprehensive explanation: *"To do this, you need to have a private key which corresponds to a certain public key or Bitcoin address. ... The person who has this private key can create a message, ... signing this message with a private key. ... Whatever you have that doesn't go into the account becomes the miner key and you sign the transaction, and then you broadcast it from your branch. ... Once the majority of the Bitcoin network sees this transaction, they are assumed valid. They [miners] will include that transaction in their next block. ... It permanently goes to the Bitcoin blockchain. ..."*

The remaining four user participants were unsure and declined to answer the question.

**Block:** We further asked our user participants to define what a block means in terms of the Bitcoin protocol and found that two users (U7 and U9) answered in sufficient detail, with U9 saying: *"A block is a computer-based structure that contains a hash of the previous block ... When a block is solved, it produces bitcoins and gives [them] to the winner or winners. They [use] a bunch of valid transactions that have occurred at that point to validate new transaction inputs... There is also a nonce within the block, as well as [a] Merkle root [e.g. root of the hash tree]... A Merkle tree [e.g. same as the hash tree] is where you have the hash value of every leaf of a tree such that in order to be certain about the completeness or the accuracy of all the descendants along one path [so] you don't need all the data on every single leaf."*

Other were not sure about the technical details: U1 and U6 commented on the block production time, with U1 saying: *"The blocks are created once every ten minutes."*; U8 said that rewards are given for finding block solutions; U4 and U10 knew that each block at least contains a hash of previous transactions. U2, U5, and U3 did not define it.

**Blockchain:** We then asked the user participants to define the blockchain: six users (U3, U4, U5, U6, U8, U10) knew that the blockchain represents a history of all transactions, with U5 explaining: *"I would assume that would be the public ledger that shows all the Bitcoin transactions and how many times transactions just confirmed. It's like the blockchain is a protocol that allows for public ledger showing transactions."*; U1, U7, and U9 said the blockchain is the accumulated blocks linking together. U2, however, posited that the "blockchain might be a string of code". Overall, user participants seemed to be more familiar with the term "blockchain" and what it represents as opposed to a block.

#### Regulation

We were curious about gauging our participants' thoughts about the government regulating the currency given the breadth of recent scandals concerning exchanges (e.g. Mt. Gox [43]) and recently proposed Bitcoin regulation by the New York State (e.g. bitlicense [20]).

Five Bitcoin users (U1, U2, U5, U8, U10) felt that the government should provide protection against fraud: U1 thought that *"the government should establish safeguards against fraud and abuse of financial institutions dealing with bitcoins."*; U5 said, *"[the government] could help people gain trust [in] Bitcoin by providing [financial] insurance. People tend to misunderstand Bitcoin because of its use on black markets, but people can do bad things with any type of money too."*

Two Bitcoin users (U4, U6) said it should not be regulated at all; U4 explained: *"The entire concept and process was developed with the intention of not having a third party especially the big brother, regulating."* Only three non-users (N2, N3, N4) responded to this question, all of them believing it should not be regulated – however, their responses were less about the core principles of Bitcoin and more about their biases towards the government. For example, N4 said: *"No, because I think they do a bad job of regulating our own money."*; N3 said, *"No. I just don't think the US government should be involved in regulating anything, pretty much."*

Two users (U3, U9) could not decide one way or the other since they thought there were both advantages and disadvantages. U7 had a clear view of what should be regulated: *"It could be that the exchange point between Bitcoin and the regular currency should be regulated. As far as regulating Bitcoin itself, I think it's a fool's errand."* He also believed that *"being able to criminalize certain actions taken with money is very useful for society."*

#### Bitcoin and Current Payment Systems

Many of the user participants compared Bitcoin to other payment methods when explaining why they preferred to use it and how they wished it to be improved. We report Bitcoin advantages and disadvantages in the following, based on the responses of our user participants.

**Transaction Benefits:** U1, U4, U5, U9, and U10 mentioned that Bitcoin has faster transaction speeds than most traditional payment methods (exempting cash for person-to-person transactions). U1 said, *"It's very efficient. It's fairly fast, faster than traditional financial systems."* U4 compared Bitcoin transactions with Western Union: *"It's almost immediate, if I was transferring money to somebody in Holland. If I was going to Western Union, paper work [needs to] go to the office, and then wait for that whole process to end on the other side. With Bitcoin, it takes a minute or two."* We should note that Bitcoin's actual transaction speed is slower than most other payment methods due to its limitations on

confirmation process and fixed block generating time. However, transferring bitcoins involves fewer steps with its peer-to-peer protocol which appears to be faster for users with international transactions.

U4, U9, and U10 mentioned that Bitcoin had lower transaction fees: U4 said, *"The fees. It costs a very, very small [amount], a couple tens of a percent for every transaction."*; U9 said, *"[Bitcoin has] low transaction fees since no processing needs to go through a third party."*

U9 and U10 also said that Bitcoin is easy to access and manage: U10 said, *"Well, I can use it basically wherever I have Internet access, whether that's my phone, my laptop, and my tablet. I can instantly send payments. People can instantly verify that I've made the payment."*

**Disadvantages of Bitcoin:** U1, U2, U5, U8, and U10 opined that Bitcoin lacks mainstream adoption. U2 said, *"Definitely the fact that not many places or companies are taking it as of now. Since it's relatively still a new concept being introduced to people in the world."*

U3 and U4 said that Bitcoin has no structure for reversing payments. U3 said, *"There are no chargebacks. It can be both an advantage and a disadvantage. Right now, [it is] really just a fact that it's so new [such that] there's not a lot that has been made available for it. This is not necessarily innovative but not fully released and insured. ..."*

U6 and U9 pointed out that the price of a bitcoin is not stable. U6 gave an illustrative example:*"If the [Bitcoin] price goes up to five thousand dollars tomorrow, then the fifty dollar toaster I bought [using bitcoins] would be the elephant in the room. Like, I could have bought a TV instead of a toaster. [I] fear of missing out on a bitcoin price increase."*

Some participants thought that using bitcoins is not as straightforward as other payment methods. U6 said it takes couple steps to set up Bitcoin transactions. Similarly, U9 said, *"You need to have quite a decent grasp of the computer and technology to be able to use this ... Everyone knows how to swipe a credit card and knows how to click buttons on PayPal but may not know what to do with private keys or what private keys even are."* However, he also believed that more people would know how to use it in the near future.

**Common Payment Methods:** As for other common payment methods, most of our participants used either credit cards (10 out of 20) or debit cards (8 out of 20) the most, with the remaining two preferring cash or checks. The main reasons for using credit cards were: convenience (U1, U7, U9, U10, N3, N4), improving credit scores (N7), delaying payments (N10), and getting reward points (U3, N9). The motivations for using debit cards, according to the participants, are: convenience (U2, U5, U6, N2, N6) and avoiding interest or fees (U4, N5, N8).

In an attempt to gauge their understanding of electronic payment methods, we asked the participants questions about the mechanics of credit cards. Most participants (18 out of 20) asserted that they understand how credit card processing works. Eight of them (U1, U2, U4, U10, N4, N6, N7, N10) explained in the context of making purchases, with U4 stating: *"I swipe it on the terminal, it's the cashier registers [sic] how much I'm to be charged on my account. Then that goes on my account and I subsequently get billed for it at the end of the month."* Three participants (U6, U7, U9) focused on explaining how merchants get money through credit cards, with U6 saying: *"On the merchant side, they have a point of sale system. They get charged per swipe. They're responsible for returning that money if there's any chargebacks."* Others explained how credit is determined: based on income levels (N3, N8) and timely payments (N5, N9, U5); the remaining discussed peripherals: interests applied when lending (U8), and payments linkable to checking accounts (N2).

When we probed participants with follow-up questions about how transactions are processed and secured without compromising privacy, they were mainly unsure. For instance, N8 said: *"To be honest with you, I'm not entirely sure where it goes after swiping through terminals..."*; N9 was not sure about the security and privacy aspects of credit cards: *"I don't know [how they design the card security]. From what I understand, there is a chip or bar code [which] is the main part of the card having my information."*

#### Money and Ideal Payment System

To gauge the participants' understanding on well-known currencies, we asked all participants what gives paper money (e.g. US dollars) its value. We found that two participants provided an accurate explanation, while others did not mention the Federal Reserve system as the key determinant.

U3 and N3 both gave a good response about the value of fiat money. U3 mentioned the Federal Reserve system being the major determinant and the acceptance by people is important as well. He said, *"It's a promissory note. That's pretty much it. The only thing that gives a value is a full faith in credit of our United States government and Reserve system, but besides that it's basically just a piece of paper. ... Stuff only work when people wanted to pay for it so that's the same with gold, gold is effectively money but it only worth because that's what people are going to pay for it. ..."* N3 emphasized the supply and demand restriction, commenting: *"Here in the United States, money gets its value by supply and demand basically. The Federal Reserve has a big impact on the value of money, and the fact that we have a country that's in good credit standing makes it more in demand than other countries in other parts of the world."*

The Federal Reserve (or the Fed), made up of 12 regional banks in major cities in the US, determines the magnitude of the money supply. The total amount of money in circulation along with available goods and services determines the actual value of paper money [2, 37]. Too much money causes inflation and not enough money causes deflation. In the United States, a small amount of inflation is preferred to motivate economic growth (e.g. 0.2% in 2015 [50]).

Other participants did not mention the Fed, the key determinant for the money supply and value. For example, U7 said, *"Money can be easily transferred between people. Visible things, functional units...all those things give money value."*

U9 and N2 believed that people give money value with N2 saying *"People. Everyone trusts it, everyone wants dollars, everyone thinks of it as valuable."* N5, N6, and N9 claimed that the things we buy give money value. In addition, U8 only mentioned: *"I would think the thing that gives US money its value is the US government."* U5 and U6 thought we just believe that the money has value, with U5 saying *"People are just believing in it. If you have money just to occur that have value yesterday. Then they are going to believe that it's going to have value tomorrow."* N8 said it is the mutual agreement between buyers and sellers that gives money value. N1, N4, N10, U1, U2, and U10 said they were unsure.

### *Ideal Payment System*

Several themes emerged when we asked all participants about what qualities an ideal payment system should have. These questions were asked prior to any questions about Bitcoin in order to avoid biasing participants.

**Faster transactions:** Four participants (U3, U5, N8, N9) pointed out that, in any case besides a person-to-person cash transaction, the current mainstream systems are slow to verify and process transactions (especially for international wire transfers), with N8 commenting: *"I would say quickness, quickness that it doesn't take forever to pay someone. If you transfer internationally, unfortunately, it was between banks and it would typically take anywhere from three or four business days to accomplish."*

**Multiple storage modalities:** U2 believed that currency should be paid from a smartphone instead of wallets. He said, *"There's a lot of applications on your phone, or tablet, that basically hold money for you and it's definitely a lot more convenient to just pay with that versus holding a wallet."* Similarly, N6 wanted a payment system that *"has both physical and electronic [elements] inside it"*. U6 also thought that a payment system should be available to view, manage, and spend with an application in the phone. What these participants described are similar to mobile payment methods such as Apple Pay [1] and Google Wallet [28].

**Increased security and privacy:** U7 and U10 said that a payment system should protect the user's privacy and personal information while guaranteeing anonymity. U4 and N8 said the transactions should be more secure and (in the words of N8): provide a *"balance between convenience and security."* N10 thought that it should deter theft, stating: *"[It should be a] currency which is not easily reusable by someone else, so the theft is controlled."* U9 mentioned Bitcoin when answering this question:*"I think the closest thing we have now to an ideal payment system or ideal currency [is] the Bitcoin form. Bitcoin has a lot of qualities that make it very well suited for a currency. There are technical aspects to how it works. It might be slightly different but it's a currency where the supply isn't controlled by any one party."*

**Increased reliability:** N9 and N4 said a system should be more reliable and have reduced opportunities for making mistakes. N9 had the experience of payment mails getting misplaced and credit cards getting lost, saying *"... The system would have to be more reliable. As long as it's a trustable source, that would be something that I would look into."*

**Lower fees:** U6, U10, N2, and N5 thought there should be less fees. N2 said, *"To me is that they don't charge me too much extra money, including transaction fees."* Also, U6 was complaining about fees imposed by bank regulators, saying, *"It shouldn't have outrageous fees to move money from one point to another. I've been transferring money from my savings to my checking account; then, I receive a notification from that bank that I've been transferring too much money between accounts and if I continue to do so, they'll charge me a fee."*

## DISCUSSION

We discuss the major findings of our study: 1) although some non-users thought not knowing how Bitcoin works was what stopped them from using it, we found our users did not need this knowledge to make transactions; 2) most user participants thought Bitcoin had good security and privacy controls despite evidence to the contrary; 3) participants highly disapproved of government regulation but still wanted governments to insure deposits; 4) participants' opinions about attributes of an ideal payment system map directly to properties that Bitcoin has; and 5) Bitcoin has barriers to overcome that make it difficult to be used for mainstream adoption.

Out of our ten non-user participants, we found that four of them had never heard about Bitcoin while the remaining six were aware of it from a superficial level based on what they had heard from the media or their social network. Many of the non-users perceived Bitcoin as being technically complicated, hard to grasp, and generally viewed it as something on-the-outside and foreign. Not surprisingly, when asked about any technical details of Bitcoin, the non-user participants expressed that they only knew about Bitcoin on a surface level (if at all) and could not answer any questions dealing with it in detail. Indeed, four non-users stated that they did not use bitcoins because they did not understand how they work.

On the other hand, we found that the user participants demonstrated a low level of comprehension about the mechanics of the Bitcoin protocol. Many of them only demonstrated a partial level of understanding when asked about topics ranging from defining components and terms of the Bitcoin system to the mining process. Some users mistakenly believed that Bitcoin has faster transaction speeds than other electronic payment methods. Bitcoin's transaction speed is highly limited by the block solution time and the amount of transactions that can be included in one block, whereas other electronic payment methods such as credit cards have much larger transaction bandwidth. On the other hand, Bitcoin usually requires fewer intermediate steps, which may effectively reduce the entire waiting time, especially for international transfers. Many of the users' descriptions of the Bitcoin protocol did not match how the protocol actually works and yet this did not prevent them from being able to buy, sell, and trade bitcoins for goods and services at various online outlets. Users were perfectly capable of using Bitcoin as well as other financial systems without needing to know the technical intricacies. This stands in contrast to what non-user participants

reported: in particular, that because they do not understand how Bitcoin works they therefore cannot use it.

Not understanding how mediums of exchange function is not an uncommon phenomenon among the general population [51]. This is also evidenced by questions we asked participants about how common electronic payment methods (e.g. credit card) work and what gives paper money value. What is curious in this scenario is that non-user participants are claiming that a lack of technical knowledge is what prevents them from adopting Bitcoin but that is not the case for other payment methods. We conjecture that this can be attributed to a few factors. First, Bitcoin is yet not easy to use or it makes potential users think that there is a lot of education required before using it. Other studies have also shown that many users perceived Bitcoin to be hard to use [3, 22]. Secondly, non-user participants do not see any important public endorsements of bitcoin as a payment method (e.g. N4 explicitly stated no motivation or need to use Bitcoin). Physical currency is the first method people are ever introduced to and is produced by governments, while electronic methods like debit and credit are promoted by banking institutions as well as vendors. Furthermore, rising digital schemes such as Google Wallet and Apple Pay are products of corporations that produce smartphone and Internet technology that pervades every aspect of daily life. Bitcoin, however, is different from these methods – it is designed to work through its peer-to-peer network, without relying on banks; but at the same time, there are no controls on the currency that insure its value or safety, and it has no universal public spokesman to make arguments for it or to advocate on its behalf. Finally, what little image it does have appears to be mostly in negative contexts among the general public. This was evidenced by our non-user participants who reported that they believed it was only used for black-market purchases, drug dealing, and money laundering. Studies on Bitcoin users have mentioned the unregulated set-up and anonymity of Bitcoin is attractive for criminal activities [58, 40], thus informing of its positive use to the general population is important.

Our user participants had several misconceptions about the security and privacy controls of Bitcoin. Most users are unconcerned with their privacy while using Bitcoin because they perceive a greater sense of control over it than they do with other payment methods and they emphasize personal responsibility in matters of security.

Many of our user participants expressed that Bitcoin inherently provides privacy since personal information is not leaked during transactions. However, it has been demonstrated through some highly rigorous deanonymization work that the opposite is actually true: the base implementation of the protocol is, at best, weakly pseudonymous. The original argument by Nakomoto is that the creation of new addresses for every transaction should protect the users' privacy. Unfortunately, this is not true: BitIodine [48], wallet clustering [42], and network traffic [35] are a sample of the methods that can be used to track user payments on the blockchain (e.g. this is the central problem of having a publicly available ledger of accounts). There are some proposals to fix the anonymity problems through mixing networks [10] and onion routing. Our user participants were mostly unaware of these.

There are no security protections built into Bitcoin to prevent fraudulent or mistaken transactions. Credits and debits to and from banking accounts can be halted or reversed with a call to the bank, but there are no such avenues with Bitcoin. As such, if money is sent to the wrong address then there is no way to reverse the transaction. There do exist some Bitcoin escrow services to mitigate this issue but none of our user participants mentioned those to us – they were either not aware of them, did not trust them either, or simply preferred that the standard Bitcoin protocol allow for reversing transactions without the use of external services. Furthermore, user participants felt that Bitcoin was overall secure despite repeated examples of bitcoin thefts (e.g. Mt. Gox, Bitstamp). However, Bitcoin is more privacy conscious than other payment methods because there is no third party that can store personal information at an intermediate step between transactions as in the case of current electronic methods.

User participants stated that they would prefer insurance for their bitcoins in the case of theft or fraud. Moreover, they said that they preferred if governments provided this as a service and claimed it would improve public trust in the currency. When followed up with questions about whether or not governments should regulate Bitcoin markets, their responses were mainly negative. This is not very practical, since allowing the government to insure deposits would give them a measure of control over users and exchanges, at which point they could then introduce side regulations by using the insurance as a cudgel in instances when they demand compliance.

We asked our participants about what features an ideal payment system should have in order for it to appeal to them. They advocated for having fast transactions, especially when dealing with international transfers. Several participants expressed discomfort with the wait time associated with using traditional wiring methods to transfer money between accounts and overseas. Participants said that they preferred to have multiple modalities for using the money – both virtual and physical representations were desired as a matter of habit and convenience. Participants also were very concerned with financial fraud and privacy. As for the transaction fee, most participants preferred it be zero or as close to zero as possible. Bitcoin satisfies some of these properties that participants advocated for: fast international transactions and low fees.

Bitcoin faces mainstream adoption problems because it does not appear to fit, based on descriptions of other payment methods by our participants, the needs of the general population. Debit, credit, and cash have all carved niches of use in day-to-day life: debit is a convenient method that draws directly from a banking account; credit can be used in instances where money is not immediately available; cash is accepted everywhere and can be transferred between people quickly. Although Bitcoin also has superior use cases (e.g. low fees, no central authority), it does not scale well in day-to-day scenarios (micropayments, intercontential money transfers, and person-to-person transactions) for the general population. As reflected from our non-user responses, people mostly avoid

using bitcoins because they do not feel the need and it is relatively new. Although it has benefits, it also has unknown risks. Given that it requires effort to get started, they tend to work around them. It is currently still a new method of payment that does not have strong appeal to users – for example, a person may not commonly use credit cards but will hold onto one to build their credit scores in the US. Bitcoin does not have such an allure.

### Implications to Design and Theory

Bitcoin, as a peer-to-peer payment system, has advantages in the form of: low transaction fees, fast global transfers, privacy, and no regulation. However, for wide adoption, it still has several limitations that need the attention of designers: its limited reputation, dynamic value, and inability to reverse payments. Interestingly, the properties that participants of both groups ascribed to an ideal payment system are ones that Bitcoin has.

One finding worth restating is that some non-users have the misconception that not knowing how Bitcoin works stops them from using it. As for typical financial systems, people care more about how to use it than how it works. Thus, it is important to find out why non-users have this misconception. Based on some of our participants responses, we believe there are several possible causes: (1) Bitcoin makes people suspicious about whether the currency can be trusted. Our participants pointed out black market usage and no chargebacks as negative aspects of the user experience. (2) Lots of Bitcoin websites and forums' discussions about Bitcoin are highly technical, which may mislead people to think that they need to understand how it works to use it. Some of our non-users mistakenly thought that mining is the only way to obtain bitcoins since they frequently found discussions about mining online. (3) The way Bitcoin is presented leads people perceive that it is not easy to use or even too scary to try out. Some clear guidelines and classifications about what is needed to know for someone who only wants to use it, someone who wants to do mining, and someone who wants to help develop would be very useful. Positive reinforcement about Bitcoin through news articles or tutorials can help the general populace correctly interpret Bitcoin.

Previous studies [39] on ideal aspects of digital payment schemes stated that there are five aspects of a digital payment system required to appeal to users: (1) reduced complexity, (2) center around public use, (3) support money management without increasing burden or degrading user experience, (4) engage multiple senses, (5) and be fun to use [39]. The last two are aspects that are very particular to the study environment, Japan, which has many digital payment schemes that vie for control of the market. As evidenced by our participant responses, we can see where Bitcoin falls short. Bitcoin does not reduce complexity, instead it increases it by asking users to manage addresses and wallets. Bitcoin is centered around public use from its first design principles (user-first, no third parties). There are various clients to manage money, however, the introduction of additional processes to use is clearly an increased burden on the user. Our questions do not cover well to the last two categories.

### Limitations

The availability and willingness of participants to participate in research can affect the results as is typical for interview studies. Many of the user participants were very privacy conscious. This makes it difficult to recruit from the Bitcoin user community. We cannot be certain how this affects our findings. Our Bitcoin user sample does not fully represent all possible actors in Bitcoin system: miners, investors, dogmatic believers, economists, computer scientists, and end users. However, our participants spanned more than seven different states across the US and varied widely in demographic terms. Thus, some future work would be warranted in characterizing the Bitcoin population. For example, how pervasive are the thoughts about Bitcoin advantages and disadvantages?

## CONCLUSIONS

We presented a study of users and non-users of Bitcoin using semi-structured interviews to discover more about their knowledge, attitudes, and opinions concerning Bitcoin. We found that many of our user participants held various misconceptions when talking about technical details. Some non-user participants thought that they could not use Bitcoin since they do not know how it works. In contrast, this is actually not a barrier for the user participants so the real reason must lie elsewhere: the way Bitcoin is presented, issues concerning user experience, privacy and security concerns, or perceptions of risk, which may require further study. The major advantages of Bitcoin, according to user participants, include fast transaction speed, low transaction fees, security, and no third-party regulation. Interestingly, while user participants staunchly oppose government regulation, they still desire them to insure any deposits.

We conclude that the Bitcoin user demographic pools are a highly fragmented collection of people that merit further examination while the non-user demographic pool could be surveyed in more detail about the barriers to entry necessary for them to use Bitcoin and other cryptocurrencies. Our paper provides suggestions for the design of Bitcoin and similar crypto-currencies for further adoption.

## ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant Numbers 1211079 and 1546689. Xianyi Gao was supported by the National Science Foundation Graduate Research Fellowship Program under Grant Number 1433187. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation. Gradeigh D. Clark was supported by the Department of Defense (DoD) through the National Defense Science and Engineering Graduate Fellowship (NDSEG) Program. We also thank Eric Wengrowski for help in the initial stages of the project.

## REFERENCES


1. Apple Pay. 2015. Apple Pay: Your wallet without the wallet. (2015). Retrieved August 22, 2015 from http://www.apple.com/apple-pay/?cid=wwa-us-kwg-features-com.
2. Roger A. Arnold. 2008. *Economics* (9th ed.). Cengage Learning, 273–278.
3. Aaron W Baur, Julian Bühler, Markus Bick, and Charlotte S Bonorden. 2015. Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co. In *Open and Big Data Management and Innovation*. Springer, 63–80.
4. Bitcointalk Forum. 2015. Bitcoin Discussion. (2015). Retrieved August 22, 2015 from https://bitcointalk.org/index.php?board=1.0.
5. Blockchain. 2015a. Block Height 367500. (29 July 2015). Retrieved September 20, 2015 from https://blockchain.info/block-height/367500.
6. Blockchain. 2015b. Number Of Users. (2015). Retrieved August 27, 2015 from https://blockchain.info/charts/my-wallet-n-users.
7. Blockchain. 2015c. Total Coins In Circulation. (2015). Retrieved August 27, 2015 from https://blockchain.info/charts/total-bitcoins.
8. Jeremiah Bohr and Masooda Bashir. 2014. Who Uses Bitcoin? An exploration of the Bitcoin community. In *Privacy, Security and Trust (PST)*. 94–101.
9. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A Kroll, and Edward W Felten. 2015. Research perspectives on bitcoin and secondgeneration cryptocurrencies. In *IEEE Symposium on Security and Privacy. IEEE*.
10. Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A Kroll, and Edward W Felten. 2014. Mixcoin: Anonymity for Bitcoin with accountable mixes. In *Financial Cryptography and Data Security*. Springer, 486–504.
11. John M. Carroll and Victoria Bellotti. 2015. Creating Value Together: The Emerging Design Space of Peer-to-Peer Currency and Exchange. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work (CSCW '15)*. ACM, New York, NY, USA, 1500–1510. http://doi.acm.org/10.1145/2675133.2675270
12. Kathy Charmaz. 2014. *Constructing Grounded Theory, 2nd Edition*. SAGE Publications Ltd.
13. David Chaum. 1983. Blind signatures for untraceable payments. In *Advances in cryptology*. Springer, 199–203.
14. Elizabeth F. Churchill. 2015. Why Should We Care About Bitcoin? *interactions* 22, 5 (Aug. 2015), 20–21. http://doi.acm.org/10.1145/2810199
15. Pavel Ciaian, Miroslava Rajcaniova, and d'Artis Kancs. 2014. The Economics of BitCoin Price Formation. *arXiv preprint arXiv:1405.4498* (2014).
16. Coinbase. 2015. Charts. (2015). Retrieved August 27, 2015 from https://coinbase.com/charts.
17. Daryl Collins, Jonathan Morduch, Stuart Rutherford, and Orlanda Ruthven. 2009. *Portfolios of the poor: how the world's poor live on $2 a day*. Princeton University Press.
18. Craigslist. 2015. Craigslist in US. (2015). Retrieved August 22, 2015 from http://www.craigslist.org/about/sites#US.
19. Michael A. Cusumano. 2014. The Bitcoin Ecosystem. *Commun. ACM* 57, 10 (Sept. 2014), 22–24. http://doi.acm.org/10.1145/2661047
20. Department of Finanial Services NY. 2015. Revised BitLicense Regulatory Framework. (2015). Retrieved December 20, 2015 from http://www.dfs.ny.gov/legal/regulations/rev_bitlicense_reg_framework.htm.
21. Jonathan Donier and Julius Friedrich Bonart. 2014. A million metaorder analysis of market impact on the Bitcoin. *Available at SSRN* (2014).
22. Shayan Eskandari, David Barrera, Elizabeth Stobert, and Jeremy Clark. 2015. A First Look at the Usability of Bitcoin Key Management. In *NDSS Workshop on Usable Security (USEC)*. http://people.inf.ethz.ch/barrerad/files/usec15-eskandari.pdf
23. David S Evans. 2014. Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms. *University of Chicago Coase-Sandor Institute for Law & Economics Research Paper* 685 (2014).
24. Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *Financial Cryptography and Data Security*. Springer, 436–454.
25. Jennifer Ferreira, Mark Perry, and Sriram Subramanian. 2015. Spending Time with Money: From Shared Values to Social Connectivity. In *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work (CSCW '15)*. ACM, New York, NY, USA, 1222–1234. http://doi.acm.org/10.1145/2675133.2675230
26. David Garcia, Claudio J Tessone, Pavlin Mavrodiev, and Nicolas Perony. 2014. The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy. *Journal of the Royal Society Interface* 11, 99 (2014), 20140623.
27. Arthur Gervais, Ghassan Karame, Srdjan Capkun, and Vedran Capkun. 2013. Is Bitcoin a decentralized currency? *IACR Cryptology ePrint Archive* 2013 (2013), 829.
28. Google Wallet. 2015. Tap and pay with your phone. (2015). Retrieved August 22, 2015 from http://www.google.com/wallet/shop-in-stores/?gclid=CKP_1JGCscMCFc0kgQodTZIACA.

29. Dominic Hobson. 2013. What is Bitcoin? *XRDS* 20, 1 (Sept. 2013), 40–44. http://doi.acm.org/10.1145/2510124
30. Tamara Holmes. 2015. Payment method statistics. (15 June 2015). Retrieved September 24, 2015 from http://www.creditcards.com/credit-card-news/payment-method-statistics-1276.php.
31. Jermain Kaminski and Peter Gloor. 2014. Nowcasting the Bitcoin Market with Twitter Signals. *arXiv preprint arXiv:1406.7577* (2014).
32. Jofish Kaye, Janet Vertesi, Jennifer Ferreira, Barry Brown, and Mark Perry. 2014b. #CHImoney: Financial Interactions, Digital Cash, Capital Exchange and Mobile Money. In *CHI '14 Extended Abstracts on Human Factors in Computing Systems (CHI EA '14)*. ACM, New York, NY, USA, 111–114. http://doi.acm.org/10.1145/2559206.2559221
33. Joseph Jofish Kaye, Mary McCuistion, Rebecca Gulotta, and David A. Shamma. 2014a. Money Talks: Tracking Personal Finances. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '14)*. ACM, New York, NY, USA, 521–530. http://doi.acm.org/10.1145/2556288.2556975
34. Dániel Kondor, Márton Pósfai, István Csabai, and Gábor Vattay. 2014. Do the rich get richer? An empirical analysis of the Bitcoin transaction network. *PloS one* 9, 2 (2014), e86197.
35. Philip Koshy, Diana Koshy, and Patrick McDaniel. 2014. An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. In *Financial Cryptography and Data Security*. 469–485.
36. Deepti Kumar, David Martin, and Jacki O'Neill. 2011. The Times They Are A-changin': Mobile Payments in India. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '11)*. ACM, New York, NY, USA, 1413–1422. http://doi.acm.org/10.1145/1978942.1979150
37. Doug Levinson. 2014. What gives a dollar bill its value? Video. (23 June 2014). Retrieved September 18, 2015 from http://ed.ted.com/lessons/what-gives-a-dollar-bill-its-value-doug-levinson.
38. Caitlin Lustig and Bonnie Nardi. 2015. Algorithmic Authority: The Case of Bitcoin. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on*. 743–752. DOI: http://dx.doi.org/10.1109/HICSS.2015.95
39. Scott Mainwaring, Wendy March, and Bill Maurer. 2008. From Meiwaku to Tokushita!: Lessons for Digital Money Design from Japan. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. ACM, New York, NY, USA, 21–24. http://doi.acm.org/10.1145/1357054.1357058
40. Bill Maurer, Taylor C Nelms, and Lana Swartz. 2013. When perhaps the real problem is money itself!: the practical materiality of Bitcoin. *Social Semiotics* 23, 2 (2013), 261–277.
41. Indrani Medhi, S.N. Nagasena Gautama, and Kentaro Toyama. 2009. A Comparison of Mobile Money-transfer UIs for Non-literate and Semi-literate Users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '09)*. ACM, New York, NY, USA, 1741–1750. http://doi.acm.org/10.1145/1518701.1518970
42. Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage. 2013. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. In *Proceedings of the 2013 Conference on Internet Measurement Conference (IMC '13)*. ACM, New York, NY, USA, 127–140. http://doi.acm.org/10.1145/2504730.2504747
43. Tyler Moore and Nicolas Christin. 2013. Beware the middleman: Empirical analysis of bitcoin-exchange risk. In *Financial Cryptography and Data Security*. Springer, 25–33.
44. Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Consulted* 1, 2012 (2008), 28.
45. Gary Pritchard, John Vines, and Patrick Olivier. 2015. Your Money's No Good Here: The Elimination of Cash Payment on London Buses. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI '15)*. ACM, New York, NY, USA, 907–916. http://doi.acm.org/10.1145/2702123.2702137
46. Reddit. 2015. Bitcoin Subreddit. (2015). Retrieved August 22, 2015 from http://www.reddit.com/r/bitcoin.
47. Simulacrum. 2013. The Demographics of Bitcoin (PART 1 UPDATED). (2013). Retrieved July 20, 2015 from http://simulacrum.cc/2013/03/04/the-demographics-of-bitcoin-part-1-updated/.
48. Michele Spagnuolo, Federico Maggi, and Stefano Zanero. 2014. Bitiodine: Extracting intelligence from the bitcoin network. In *Financial Cryptography and Data Security*. Springer, 457–468.
49. Janet Stocks, Capitolina Díaz, and Björn Halleröd. 2007. *Modern couples sharing money, sharing life*. Palgrave Macmillan.
50. Joana Taborda. 2015. United States Inflation Rate. (16 September 2015). Retrieved September 20, 2015 from http://www.tradingeconomics.com/united-states/inflation-cpi.
51. Pater Tenebrarum. 2015. Misconceptions About Gold. (16 February 2015). Retrieved December 20, 2015 from http://www.acting-man.com/?p=35868.
52. Marshall Van Alstyne. 2014. Why Bitcoin Has Value. *Commun. ACM* 57, 5 (May 2014), 30–32. http://doi.acm.org/10.1145/2594288

53. Vericoin. 2015. The VeriCoin Android wallet featuring VeriBit. (2015). Retrieved August 22, 2015 from http://www.vericoin.info/.

54. John Vines, Mark Blythe, Paul Dunphy, and Andrew Monk. 2011. Eighty something: banking for the older old. In *Proceedings of the 25th BCS Conference on Human-Computer Interaction*. British Computer Society, 64–73.

55. John Vines, Mark Blythe, Paul Dunphy, Vasillis Vlachokyriakos, Isaac Teece, Andrew Monk, and Patrick Olivier. 2012a. Cheque Mates: Participatory Design of Digital Payments with Eighty Somethings. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '12)*. ACM, New York, NY, USA, 1189–1198. http://doi.acm.org/10.1145/2207676.2208569

56. John Vines, Paul Dunphy, Mark Blythe, Stephen Lindsay, Andrew Monk, and Patrick Olivier. 2012b. The Joy of Cheques: Trust, Paper and Eighty Somethings. In *Proceedings of the ACM 2012 Conference on Computer Supported Cooperative Work (CSCW '12)*. ACM, New York, NY, USA, 147–156. http://doi.acm.org/10.1145/2145204.2145229

57. Yang Wang and Scott D. Mainwaring. 2008. Human-Currency Interaction: Learning from Virtual Currency Use in China. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '08)*. ACM, New York, NY, USA, 25–28. http://doi.acm.org/10.1145/1357054.1357059

58. Aaron Yelowitz and Matthew Wilson. 2015. Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters* 22, 13 (2015), 1030–1036. DOI: http://dx.doi.org/10.1080/13504851.2014.995359

59. Viviana Zelizer. 1997. *The social meaning of money: Pin money, paychecks, poor relief and other currencies*. Princeton University Press. Princeton.