A fistful of bitcoins: characterizing payments among men with no names

Conference Paper · October 2013

DOI: 10.1145/2504730.2504747

CITATIONS
367

READS
703

7 authors, including:

Marjori Pomarole

4 PUBLICATIONS **603** CITATIONS

SEE PROFILE

Damon Mccoy

New York University

63 PUBLICATIONS **4,508** CITATIONS

SEE PROFILE

A Fistful of Bitcoins: Characterizing Payments Among Men with No Names

Sarah Meiklejohn Marjori Pomarole Grant Jordan
Kirill Levchenko Damon McCoy[†] Geoffrey M. Voelker Stefan Savage

University of California, San Diego George Mason University[†]

ABSTRACT

Bitcoin is a purely online virtual currency, unbacked by either physical commodities or sovereign obligation; instead, it relies on a combination of cryptographic protection and a peer-to-peer protocol for witnessing settlements. Consequently, Bitcoin has the unintuitive property that while the ownership of money is implicitly anonymous, its flow is globally visible. In this paper we explore this unique characteristic further, using heuristic clustering to group Bitcoin wallets based on evidence of shared authority, and then using re-identification attacks (i.e., empirical purchasing of goods and services) to classify the operators of those clusters. From this analysis, we characterize longitudinal changes in the Bitcoin market, the stresses these changes are placing on the system, and the challenges for those seeking to use Bitcoin for criminal or fraudulent purposes at scale.

Categories and Subject Descriptors

K.4.4 [**Electronic Commerce**]: Payment schemes

Keywords

Bitcoin; Measurement; Anonymity

1. INTRODUCTION

Demand for low friction e-commerce of various kinds has driven a proliferation in online payment systems over the last decade. Thus, in addition to established payment card networks (e.g., Visa and Mastercard) a broad range of so-called "alternative payments" has emerged including eWallets (e.g., Paypal, Google Checkout, and WebMoney), direct debit systems (typically via ACH, such as eBillMe), money transfer systems (e.g., Moneygram) and so on. However, virtually all of these systems have the property that they are denominated in existing fiat currencies (e.g., dollars), explicitly identify the payer in transactions, and are centrally or quasi-centrally administered.[1]

By far the most intriguing exception to this rule is Bitcoin. First deployed in 2009, Bitcoin is an independent online monetary system that combines some of the features of cash and existing online payment methods. Like cash, Bitcoin transactions do not explicitly identify the payer or the payee: a transaction is a cryptographically-signed transfer of funds from one public key to another. Moreover, like cash, Bitcoin transactions are irreversible (in particular, there is no *chargeback* risk as with credit cards). However, unlike cash, Bitcoin requires third party mediation: a global peer-to-peer network of participants validates and certifies all transactions; such decentralized accounting requires each network participant to maintain the entire transaction history of the system, currently amounting to over 3GB of compressed data. Bitcoin identities are thus *pseudo-anonymous*: while not explicitly tied to real-world individuals or organizations, all transactions are completely transparent.[2]

This unusual combination of features has given rise to considerable confusion about the nature and consequences of the anonymity that Bitcoin provides. In particular, there is concern that the combination of scalable, irrevocable, anonymous payments would prove highly attractive for criminals engaged in fraud or money laundering. In a widely leaked 2012 Intelligence Assessment, FBI analysts make just this case and conclude that a key "advantage" of Bitcoin for criminals is that "law enforcement faces difficulties detecting suspicious activity, identifying users and obtaining transaction records" [7]. Similarly, in a late 2012 report on Virtual Currency Schemes, the European Central Bank opines that the lack of regulation and due diligence might enable "criminals, terrorists, fraudsters and money laundering" and that "the extent to which any money flows can be traced back to a particular user is unknown" [6]. Indeed, there is at least some anecdotal evidence that this statement is true, with the widely publicized "Silk Road" service using Bitcoin to trade in a range of illegal goods (e.g., restricted drugs and firearms). Finally, adding to this urgency is Bitcoin's considerable growth, both quantitatively — a merchant servicer, Bitpay, announced that it had signed up over 1,000 merchants in 2012 to accept the currency, and in April 2013 the exchange rate soared to 235 USD per bitcoin before settling to a more modest 100 USD per bitcoin — and qualitatively via integration with existing payment mechanisms (e.g., Bitinstant offering to tie users' Bitcoin wallets to Mastercard accounts [5] and Bitcoin Central's recent partnership with the French bank Crédit Mutuel Arkéa to gateway Bitcoin into the banking system [16]) and the increasing attention of world financial institutions (e.g., Canada's recent decision to tax Bitcoin transactions [3] and FinCEN's recent regulations

[1] In particular, there is a central controlling authority who has the technical and legal capacity to tie a transaction back to a pair of individuals.

[2] Note that this statement is not strictly true since private exchanges of Bitcoin between customers of a single third party exchange, such as Mt. Gox, need not (and do not) engage the global Bitcoin protocol and are therefore not transparent.

IMC'13, October 23–25, 2013, Barcelona, Spain.

http://dx.doi.org/10.1145/2504730.2504747.

on virtual currencies [8]). In spite of this background of intense interest, Bitcoin's pseudo-anonymity has limited how much is known about how the currency is used and how Bitcoin's use has evolved over time.

In this context, our work seeks to better understand the traceability of Bitcoin flows and, through this understanding, explore the evolution in how Bitcoin has been used over time. Importantly, our goal is not to generally de-anonymize all Bitcoin users — as the abstract protocol design itself dictates that this should be impossible — but rather to identify certain *idioms of use* present in concrete Bitcoin network implementations that erode the anonymity of the users who engage in them. Our approach is based on the availability of the Bitcoin *block chain*: a replicated graph data structure that encodes all Bitcoin activity, past and present, in terms of the public digital signing keys party to each transaction. However, since each of these keys carries no explicit information about ownership, our analysis depends on imposing additional structure on the transaction graph.

Our methodology has two phases. First, in Section 3, we describe a re-identification attack wherein we open accounts and make purchases from a broad range of known Bitcoin merchants and service providers (e.g., Mt. Gox and Silk Road). Since one endpoint of the transaction is known (i.e., we know which public key we used), we are able to positively label the public key on the other end as belonging to the service; we augment this attack by crawling Bitcoin forums for "self-labeled" public keys (e.g., where an individual or organization explicitly advertises a key as their own). Next, in Section 4, we build on past efforts [2, 17, 18, 21] to cluster public keys based on evidence of shared spending authority. This clustering allows us to amplify the results of our re-identification attack: if we labeled one public key as belonging to Mt. Gox, we can now transitively taint the entire cluster containing this public key as belonging to Mt. Gox as well. The result is a condensed graph, in which nodes represent entire users and services rather than individual public keys.

From this data we characterize Bitcoin use longitudinally, focusing in particular on the evolution of services and their role in the Bitcoin network. Finally, in Section 5, we combine what we have learned to examine the suitability of Bitcoin for hiding large-scale illicit transactions. Using the dissolution of a large Silk Road wallet and notable Bitcoin thefts as case studies, we demonstrate that an agency with subpoena power would be well placed to identify who is paying money to whom. Indeed, we argue that the increasing dominance of a small number of Bitcoin institutions (most notably services that perform currency exchange), coupled with the public nature of transactions and our ability to label monetary flows to major institutions, ultimately makes Bitcoin unattractive today for high-volume illicit use such as money laundering.

2. BITCOIN BACKGROUND

Our heuristics that we use to cluster addresses depend on the structure of the Bitcoin protocol, so we first describe it here, and briefly mention the anonymity that it is intended to provide. Additionally, much of our analysis discusses the "major players" and different categories of bitcoin-based services, so we also present a more high-level overview of Bitcoin participation, as well as some general statistics about the Bitcoin network.

2.1 Bitcoin protocol description

Bitcoin is a decentralized electronic currency, introduced by (the pseudonymous) Satoshi Nakamoto in 2008 [15] and deployed on January 3 2009. Briefly, a bitcoin[3] can be thought of as a chain of *transactions* from one owner to the next, where owners are identified by a *public key* (in practice, a public key for the ECDSA signature scheme) that serves as a pseudonym; i.e., users can use any number of public keys and their activity using one set of public keys is not inherently tied to their activity using another set, or to their real-world identity (so that, e.g., a user can use a different public key to deposit bitcoins into his Silk Road account than to withdraw bitcoins from his Mt. Gox account, and expect that these activities cannot be linked to either his real identity or to each other). In each transaction, the previous owner signs — using the secret signing key corresponding to his public key — a hash of the transaction in which he received the bitcoins (in practice, a SHA-256 hash) and the public key of the next owner. This signature (i.e., transaction) can then be added to the set of transactions that constitutes the bitcoin; because each of these transactions references the previous transaction (i.e., in sending bitcoins, the current owner must specify where they came from), the transactions form a chain. To verify the validity of a bitcoin, a user can check the validity of each of the signatures in this chain.

To prevent double spending, it is necessary for each user in the system to be aware of all such transactions. Double spending can then be identified when a user attempts to transfer a bitcoin after he has already done so. To determine which transaction came first, transactions are grouped into *blocks*, which serve to timestamp the transactions they contain and vouch for their validity. Blocks are themselves formed into a chain, with each block referencing the previous one (and thus further reinforcing the validity of all previous transactions). This process yields a *block chain*, which is then publicly available to every user within the system.

This process describes how to transfer bitcoins and broadcast transactions to all users of the system. Because Bitcoin is decentralized and there is thus no central authority minting bitcoins, we must also consider how bitcoins are generated in the first place. In fact, this happens in the process of forming a block: each accepted block (i.e., each block incorporated into the block chain) is required to be such that, when all the data inside the block is hashed, the hash begins with a certain number of zeroes. To allow users to find this particular collection of data, blocks contain, in addition to a list of transactions, a *nonce*. (We simplify the description slightly to ease presentation.) Once someone finds a nonce that allows the block to have the correctly formatted hash, the block is then broadcast in the same peer-to-peer manner as transactions. The system is designed to generate only 21 million bitcoins in total. Finding a block currently comes with an attached reward of 25 BTC; this rate was 50 BTC until November 28 2012 (block height 210,000), and is expected to halve again in 2016, and eventually drop to 0 in 2140.

In summary, the dissemination of information within the Bitcoin network is as follows (and as depicted in Figure 1): first, users generate at least one signing keypair, and publicize the public key, or *address* — in the rest of the paper we use these terms interchangeably — to receive bitcoins (and again, users can choose to use a single public key or arbitrarily many). If a user has bitcoins that she wishes to transfer, she broadcasts a *transaction*, proving that she has the bitcoins and indicating the address of the recipient to her peers, who in turn broadcast it to their peers. Eventually, this transaction reaches a miner, who collects the transactions he hears about into a *block*, and works on finding the right data/nonce bal-

[3]Following established convention, we use the capitalized term *Bitcoin* when referring to the payment system and peer-to-peer network and the lowercase term *bitcoin* (abbreviated *BTC*), when referring to the unit of currency.

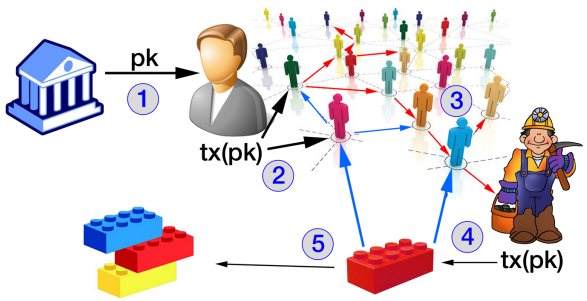


Figure 1: The main players in the Bitcoin landscape. In (1), a user wishing to deposit bitcoins into a bank receives a *public key*, or *address*, belonging to the bank. In (2), the user incorporates both his own public key and the one sent to him by the bank into a *transaction*, which he then broadcasts to his peers. In (3), the transaction floods the network. In (4), the transaction is eventually received by a *miner*, who works to incorporate the transaction into a *block*. In (5), this block is then flooded through the network, and in this way is incorporated into the global *block chain*. The bitcoins now belong to the public key of the bank, and thus have been successfully deposited.

ance to hit the target hash. He also includes in the block a special *coin generation* transaction that specifies his address for receiving the block reward. Finally, when the miner does find such a block, he broadcasts it to his peers, who again broadcast it to their peers. As his reward, the block reward and all the fees for the included transactions are credited to his specified address. When another block has been formed, referencing his block as the previous block, his block can now be considered part of the *block chain*.

2.2 Participants in the Bitcoin network

In practice, the way in which Bitcoin can be used is much simpler than the above description might indicate. First, generating a block is so computationally difficult that very few individual users attempt it on their own. Instead, users may join a *mining pool* such as Deepbit, in which they contribute "shares" to narrow down the search space, and earn a small amount of bitcoins in exchange for each share.

Users may also avoid coin generation entirely, and simply purchase bitcoins through one of the many *exchanges*, such as Mt. Gox. They may then keep the bitcoins in a wallet stored on their computer or, to make matters even easier, use one of the many *wallet services* (i.e., banks) that exist online (although the two most popular of these, MyBitcoin and Instawallet, have both shut down due to thefts).

Finally, to actually spend their bitcoins, users could gamble with one of the popular dice games such as Satoshi Dice. They could also buy items from various online vendors, such as Bitmit ("the eBay of Bitcoin"), the notorious Tor-based service Silk Road, or with vendors, such as Wordpress, that might ordinarily accept only US dollars but accept bitcoins through BitPay, a payment gateway that takes bitcoins from the buyer but offers the option of payment in USD to the seller (thus eliminating all Bitcoin-based risk for the vendor). Finally, users wishing to go beyond basic currency speculation can invest their bitcoins with firms such as Bitcoinica (shut down after a series of thefts) or Bitcoin Savings & Trust (later revealed as a major Ponzi scheme). In Section 3, we more fully describe the role and impact of these and other services within the Bitcoin network.

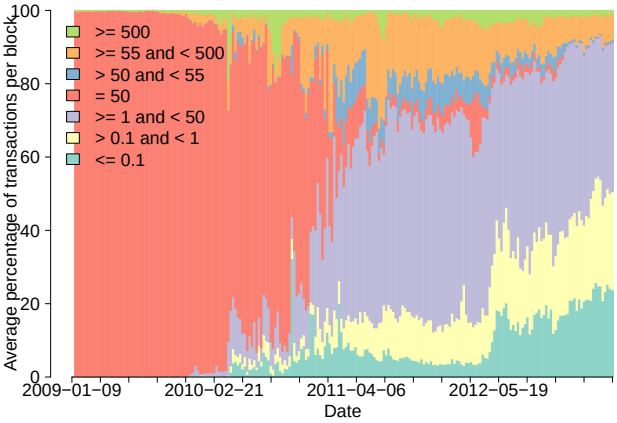


Figure 2: The distribution, over time and averaged weekly, of transaction values. The plot and legend both run, bottom to top, from the smallest-valued transactions to the highest.

2.3 Bitcoin network statistics

We used the `bitcoind` client to download the block chain, and parsed it into a PostgreSQL database using a modified version of the `bitcointools` library developed by Gavin Andresen [1]. We last parsed the block chain on April 13 2013, when there were 231,207 blocks, containing 16,086,073 transactions and 12,056,684 distinct public keys.

To begin, we looked at the size of transactions; i.e., the number of bitcoins sent in a transaction. Figure 2 depicts the changing percentage of various transaction sizes over time. Not surprisingly, until approximately April 2010 — the first 15 months that Bitcoin was deployed — almost all transactions involved exactly 50 bitcoins (the initial reward for mining a block), and indeed these transactions became a minority of all transactions only in January 2011. This activity reflects the adoption phase of Bitcoin, in which most blocks contained the coin generation transaction and nothing more. (In later phases, the mining reward is likely a little more than 50 because it includes miner fees, which is why we created a separate bin for values between 50 and 55.) We also see a second turning point in early 2012, in which the percentage of transactions carrying less than a single bitcoin in total value doubled abruptly (from 20% to 40%), while the percentage of transactions carrying less than 0.1 BTC tripled.

We also observed how quickly bitcoins were spent; i.e., once they were received, how long did it take the recipient to spend them? Figure 3 shows breakdowns both in terms of public keys (how many recipient public keys spent their contents in a certain time window) and in terms of value (how many of the bitcoins that were received were spent in a certain time window).

Looking at this figure, we again see two clear turning points. The first, in early 2011, represents a point at which users began meaningfully spending bitcoins, rather than just "hoarding" them; in fact, from this point on a negligible fraction of bitcoins are hoarded. Nevertheless, these early hoarders in fact took most of the bitcoins out of circulation; as observed by Ron and Shamir [18], a significant majority of all bitcoins are in these "sink" addresses that have to date never spent their contents (at the time they parsed the block chain it was 75%, whereas we observed it to be 64%), meaning only 4 million bitcoins are currently in circulation. Nevertheless, these remaining coins are circulating quite actively, as seen in the second turning point in Figure 3: in April 2012, the percentage of bitcoins being spent *immediately* (i.e., in the same block in which

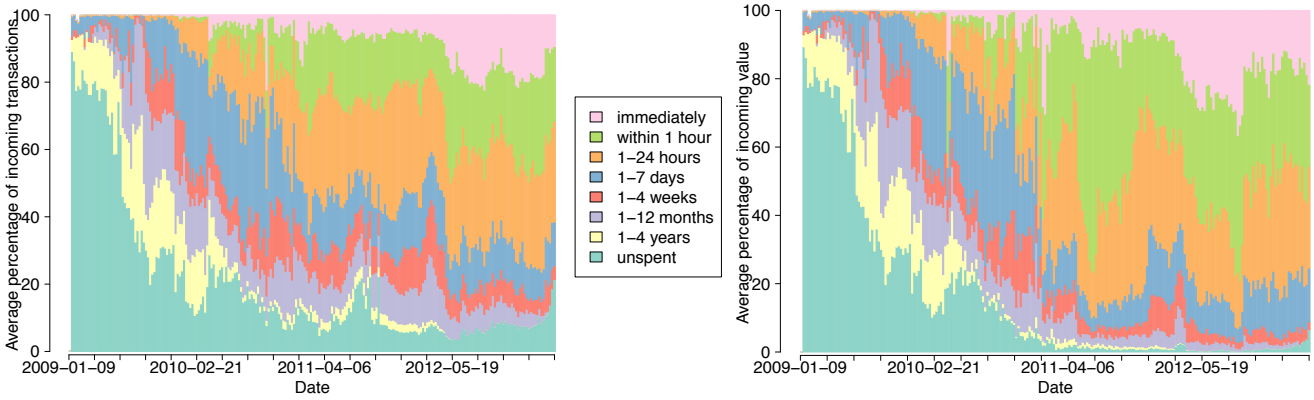


Figure 3: The trend, over time and averaged weekly, of how long public keys hold on to the bitcoins received. The plot on the left shows the percentage over all public keys, and the plot on the right shows the percentage over all value transacted. The values run bottom to top, from longest to spend (unspent as of now) to shortest to spend (spent within the same block).

they were received) doubled, and more generally half of all bitcoins are now spent within an hour of being received and 80% of bitcoins are spent within a day.

As it turns out, and as we see in Section 5.1, both these recent trends of smaller transactions and faster spending can be largely attributed to a single service: the gambling site Satoshi Dice. Thus, even a longitudinal study of the Bitcoin network already makes clear the effect that services have on current Bitcoin usage.

3. DATA COLLECTION

To identify public keys belonging to the types of services mentioned in Section 2.2, we sought to "tag" as many addresses as possible; i.e., label an address as being definitively controlled by some known real-world user (e.g., Mt. Gox or Instawallet). As we will see in Section 4.3, by clustering addresses based on evidence of shared control, we can bootstrap off the minimal ground truth data this provides to tag entire clusters of addresses as also belonging to that user.

Our predominant method for tagging users was simply transacting with them (e.g., depositing into and withdrawing bitcoins from Mt. Gox) and then observing the addresses they used; additionally, we collected known (or assumed) addresses that we found in various forums and other Web sites, although we regarded this latter kind of tagging as less reliable than our own observed data.

3.1 From our own transactions

We engaged in 344 transactions with a wide variety of services, listed in Table 1, including mining pools, wallet services, bank exchanges, non-bank exchanges, vendors, gambling sites, and miscellaneous services.

Mining pools. We attempted to mine with each of the major mining pools (a pie chart depicting the relative productivity of mining pools can be found at `blockorigin.pfoe.be/chart.php`). To do this, we used an AMD Radeon HD 7970, capable of approximately 530 million SHA-256 computations per second; this effort allowed us to trigger a payout of at least 0.1 BTC (often the minimum payout for pools) with 11 different pools, anywhere from 1 to 25 times. For each payout transaction, we then labeled the input public keys as belonging to the pool. One of these pools, Eligius, split the coin among the miners immediately upon being mined, and we were thus unable to tag any of their public keys using this method.

Wallets. We kept money with most of the major wallet services (10 in total), and made multiple deposit and withdrawal transactions for each. Three of these services — My Wallet, Easycoin, and Strongcoin — kept the funds of their users separate, which meant we were unable to link many addresses together for them.

Bank exchanges. Most of the real-time trading exchanges (i.e., in which the exchange rate is not fixed) also function as banks. As such, we tagged these services just as we did the wallets: by depositing into and withdrawing from our accounts (but rarely participating in any actual currency exchange). We kept accounts with 18 such exchanges in total.

Non-bank exchanges. In contrast, most of the fixed-rate exchanges did not function as banks, and are instead intended for one-time conversions. We therefore were able to participate in fewer transactions with these exchanges, although we again tried to transact with most of the major ones at least once (8 in total).

Vendors. We purchased goods, both physical and digital, from a wide variety of vendors. Some of the vendors, such as Bitmit and CoinDL, function more as marketplaces (the "eBay" and "iTunes" of the Bitcoin economy, respectively), while others were individual merchants. Although we purchased from Etsy, they do not provide a Bitcoin payment interface and we instead negotiated individually with the merchant. Many of the vendors we interacted with did not use an independent method for accepting bitcoins, but relied instead on the BitPay payment gateway (and one used WalletBit as a payment gateway). We also kept a wallet with Silk Road, which allowed us to tag their public keys without making any purchases. Figure 4 depicts all of our physical purchases.

Gambling. We kept accounts with five poker sites, and transacted with eight sites offering mini-games and/or lotteries. Many of the dice games (Satoshi Dice, BTC Dice, etc.) advertised their public keys, so we did fewer transactions with these services.

Miscellaneous. Four of the additional services we interacted with were *mix* or *laundry* services: when provided with an output address, they promised to send to that address coins that had no association with the ones sent to them; the more sophisticated ones offered to spread the coins out over various transactions and over time. One of these, BitMix, simply stole our money, while Bitcoin Laundry twice sent us our own coins back, indicating we were possibly their only customer at that time. We also interacted with Bit Visitor, a site that paid users to visit certain sites; Bitcoin Advertisers, which provided online advertising; CoinAd, which gave out free bitcoins; Coinapult, which forwarded bitcoins to an email ad-

Mining		
50 BTC	BTC Guild	Itzod
ABC Pool	Deepbit	Ozcoin
Bitclockers	EclipseMC	Slush
Bitminter	Eligius	
Wallets		
Bitcoin Faucet	Easywallet	Strongcoin
My Wallet	Flexcoin	WalletBit
Coinbase	Instawallet	
Easycoin	Paytunia	
Exchanges		
Bitcoin 24	BTC-e	Aurum Xchange
Bitcoin Central	CampBX	BitInstant
Bitcoin.de	CA VirtEx	Bitcoin Nordic
Bitcurex	ICBit	BTC Quick
Bitfloor	Mercado Bitcoin	FastCash4Bitcoins
Bitmarket	Mt Gox	Lilion Transfer
Bitme	The Rock	Nanaimo Gold
Bitstamp	Vircurex	OKPay
BTC China	Virwox	
Vendors		
ABU Games	BTC Buy	HealthRX
Bitbrew	BTC Gadgets	JJ Games
Bitdomain	Casascius	NZBs R Us
Bitmit	Coinabul	Silk Road
Bitpay	CoinDL	WalletBit
Bit Usenet	Etsy	Yoku
Gambling		
Bit Elfin	BitZino	Gold Game Land
Bitcoin 24/7	BTC Griffin	Satoshi Dice
Bitcoin Darts	BTC Lucky	Seals with Clubs
Bitcoin Kamikaze	BTC on Tilt	
Bitcoin Minefield	Clone Dice	
Miscellaneous		
Bit Visitor	Bitfog	CoinAd
Bitcoin Advertisers	Bitlaundry	Coinapult
Bitcoin Laundry	BitMix	Wikileaks

Table 1: The various services we interacted with, grouped by (approximate) type.

dress, where they could then be redeemed; and finally, Wikileaks, with whom we donated to both their public donation address and two one-time addresses generated for us via their IRC channel.

3.2 From other sources

In addition to our own transactions, many users publicly claim their own addresses; e.g., charities providing donation addresses, or LulzSec claiming their address on Twitter. While we did not attempt to collect all such instances, many of these tags are conveniently collected at `blockchain.info/tags`, including both addresses provided in users' signatures for Bitcoin forums, as well as self-submitted tags. We collected all of these tags — over 5,000 in total — keeping in mind that the ones that were not self-submitted (and even the ones that were) could be regarded as less reliable than the ones we collected ourselves.

Finally, we searched through the Bitcoin forums (in particular, `bitcointalk.org`) looking for addresses associated with major thefts, or now-defunct services such as Tradehill and GLBSE. Again, these sources are less reliable, so we consequently labeled users only for addresses for which we could gain some confidence through manual due diligence.

Figure 4: The physical items we purchased with bitcoins, including silver quarters from Coinabul, coffee from Bitcoin Coffee, and a used Boston CD from Bitmit. The items in green were purchased from CoinDL; in blue from Bitmit; and in red using the payment gateway BitPay.

4. ACCOUNT CLUSTERING HEURISTICS

In this section, we present two heuristics for linking addresses controlled by the same user, with the goal of collapsing the many public keys seen in the block chain into larger entities. The first heuristic, in which we treat different public keys used as inputs to a transaction as being controlled by the same user, has already been used and explored in previous work, and exploits an inherent property of the Bitcoin protocol. The second is new and based on so-called *change addresses*; in contrast to the first, it exploits a current *idiom of use* in the Bitcoin network rather than an inherent property. As such, it is less robust in the face of changing patterns within the network, but — as we especially see in Section 5.2 — it provides insight into the current Bitcoin network that the first heuristic does not.

4.1 Defining account control

Before we present our heuristics, we clarify what the results of our clustering algorithms imply; in particular, we must define what we mean by address *control*. Put simply, we say that the controller of an address is the entity (or in exceptional cases multiple entities) that is expected to participate in transactions involving that address. While this requirement implies a priori that the controller of an address knows the corresponding private key (recall that transactions are signatures, and thus knowledge of the signing key is necessary to form a valid transaction), knowledge of the private key is not a sufficient requirement for control. Consider, for example, buying physical bitcoins from a vendor such as Casascius. To form the physical bitcoin to send to you, Casascius must know the private key. Then, once you receive the bitcoin, you also learn the private key. Finally, if you redeem this private key with a service such as Mt. Gox, that service also learns the private key. In such a case, control defined solely by knowledge of the secret key is therefore not well defined.

In the above case, however, the controller of the address is in fact quite clear: as you redeemed the private key with Mt. Gox

and thus stored any bitcoins inside with them, the expected entity responsible for forming transactions on behalf of that address is Mt. Gox (otherwise, if you plan to form your own transactions, why store your money with them?).

Finally, we emphasize that our definition of address control is quite different from account *ownership*; for example, we consider a wallet service such as Instawallet to be the controller of each of the addresses it generates, even though the funds in these addresses are owned by a wide variety of distinct users.

4.2 Graph structure and definitions

To define our heuristics formally, we consider two important directed graph structures for the Bitcoin network: a transaction graph and a public key graph. In the former, vertices represent transactions, and a directed edge from a transaction t_1 to a transaction t_2 indicates that an output of t_1 was used as an input in t_2. Using this graph, we define in degrees and out degrees for transactions, which correspond exactly to the in and out degrees in the graph (i.e., the number of edges incident to and from the node, respectively).

DEFINITION 4.1. *The* in degree *for a transaction t, denoted by* $d^+_{\mathsf{tx}}(t)$*, is the number of inputs for the transaction. The* out degree *for a transaction t, denoted by* $d^-_{\mathsf{tx}}(t)$*, is the number of outputs for the transaction.*

We can also construct a graph using public keys, in which vertices are public keys and directed edges again represent the flow of money from one public key to another; here, however, the in degree of a public key reflects the number of inputs to the transaction in which it received bitcoins, so a public key that received bitcoins only once could have an in degree of (for example) five. For our purposes, we would instead like the in degree of the output public keys to be independent of how many public keys are provided as input to the transaction. We therefore define, rather than in/out degree, the *in/out count* for a public key.

DEFINITION 4.2. *The* in count *for a public key* pk*, denoted* $d^+_{\mathsf{addr}}(\mathsf{pk})$*, is the number of times* pk *has been an output in a transaction. The* out count *for a public key* pk*, denoted* $d^-_{\mathsf{addr}}(\mathsf{pk})$*, is the number of times* pk *has been an input in a transaction.*

One of the defining features of the Bitcoin protocol is the way that bitcoins must be spent. When the bitcoins redeemed as the output of a transaction are spent, they must be spent all at once: the only way to divide them is through the use of a *change address*, in which the excess from the input address is sent back to the sender. A public key can therefore spend money only as many times as it has received money (again, because each time it spends money it must spend all of it at once).

4.3 Our heuristics

Heuristic 1.

The first heuristic we use, in which we link input addresses together, has already been used many times in previous work [2, 17, 18, 21]; for completeness, we nevertheless present it here. Briefly, if two (or more) public keys are used as inputs to the same transaction, then we say that they are controlled by the same user.

HEURISTIC 1. *If two (or more) addresses are inputs to the same transaction, they are controlled by the same user; i.e., for any transaction t, all* $\mathsf{pk} \in \mathsf{inputs}(t)$ *are controlled by the same user.*

The effects of this heuristic are transitive and extend well beyond the inputs to a single transaction; e.g., if we observed one transaction with addresses A and B as inputs, and another with addresses B and C as inputs, then we conclude that A, B, and C all belonged to the same user. It is also quite safe: the sender in the transaction must know the private signing key belonging to each public key used as an input, so it is unlikely that the collection of public keys are controlled by multiple entities (as these entities would need to reveal their private keys to each other).

Using this heuristic, we partitioned the network into 5,579,176 clusters of users. By naming these clusters — using the data collection described in Section 3 — we observed that some of them corresponded to the same user; e.g., there were 20 clusters that we tagged as being controlled by Mt. Gox. (This is not surprising, as many big services appear to spread their funds across a number of distinct accounts to minimize the risk in case any one gets compromised.) This cross-cluster naming was nevertheless not too common, and we thus ended up with 5,577,481 distinct clusters (recall we started with 12,056,684 public keys). Factoring in "sink" addresses that have to date never sent any bitcoins (and thus did not get clustered using this heuristic) yields at most 6,595,564 distinct users, although we consider this number a quite large upper bound.

Heuristic 2.

Although Heuristic 1 already yields a useful clustering of users, restricting ourselves to only this heuristic does not tell the whole story. To further collapse users, our second heuristic focuses on the role of change addresses within the Bitcoin system. A similar heuristic was explored by Androulaki et al. [2] (who called them "shadow" addresses), although there are a number of important differences. In particular, their definition of shadow addresses relied upon assumptions that may have held at the time of their work, but no longer hold at present. For example, they assumed that users rarely issue transactions to two different users, which is a frequent occurrence today (e.g., payouts from mining pools, or bets on gambling sites).

As discussed above, change addresses are the mechanism used to give money back to the input user in a transaction, as bitcoins can be divided only by being spent. In one idiom of use, the change address is created internally by the Bitcoin client and never re-used; as such, a user is unlikely to give out this change address to other users (e.g., for accepting payments), and in fact might not even know the address unless he inspects the block chain. If we can identify change addresses, we can therefore potentially cluster not only the input addresses for a transaction (according to Heuristic 1) but also the change address and the input user.

Because our heuristic takes advantage of this idiom of use, rather than an inherent property of the Bitcoin protocol (as Heuristic 1 does), it does lack robustness in the face of changing (or adversarial) patterns in the network. Furthermore, it has one very negative potential consequence: falsely linking even a small number of change addresses might collapse the entire graph into large "superclusters" that are not actually controlled by a single user (in fact, we see this exact problem occur in Section 4.5). We therefore focused on designing the safest heuristic possible, even at the expense of losing some utility by having a high false negative rate, and acknowledge that such a heuristic might have to be redesigned or ultimately discarded if habitual uses of the Bitcoin protocol change significantly.

Working off the assumption that a change address has only one input (again, as it is potentially unknown to its owner and is not re-used by the client), we first looked at the outputs of every transaction. If only one of the outputs met this pattern, then we identified that output as the change address. If, however, multiple outputs had only one input and thus the change address was ambiguous, we did not label any change address for that transaction. We also avoided

certain transactions; e.g., in a coin generation, none of the outputs are change addresses.

In addition, in custom usages of the Bitcoin protocol it is possible to specify the change address for a given transaction. Thus far, one common usage of this setting that we have observed has been to provide a change address that is in fact the same as the input address.[4] We thus avoid such "self-change" transactions as well.

DEFINITION 4.3. *A public key* pk *is a* one-time change address *for a transaction* t *if the following conditions are met:*

1. $d^{+}_{\mathsf{addr}}(\mathsf{pk}) = 1$*; i.e., this is the first appearance of* pk.
2. *The transaction* t *is not a coin generation.*
3. *There is no* $\mathsf{pk}' \in \mathsf{outputs}(t)$ *such that* $\mathsf{pk}' \in \mathsf{inputs}(t)$*; i.e., there is no self-change address.*
4. *There is no* $\mathsf{pk}' \in \mathsf{outputs}(t)$ *such that* $\mathsf{pk}' \neq \mathsf{pk}$ *but* $d^{+}_{\mathsf{addr}}(\mathsf{pk}') = 1$*; i.e., for all the outputs in the transaction, condition* 1 *is met for only* pk.

HEURISTIC 2. *The one-time change address is controlled by the same user as the input addresses; i.e., for any transaction* t*, the controller of* $\mathsf{inputs}(t)$ *also controls the one-time change address* $\mathsf{pk} \in \mathsf{outputs}(t)$ *(if such an address exists).*

4.4 The impact of change addresses

To see the impact of change addresses on user clustering, consider the following illustrative example: suppose we want to measure the *incoming value* of the major services with whom we interacted; i.e., we want to know how many bitcoins they received over time. If we consider the incoming value of services across seven different categories — exchanges that function as banks, mining pools, wallet services, gambling sites, vendors, fixed-rated exchanges that do not function as banks, and investment schemes — then, using Heuristic 1, we obtain the results shown in Figure 5a.

Looking at Figure 5a cumulatively, we might first notice that, for the past year and a half, the major users we tagged account for anywhere from 20% to 40% of the total incoming value. Comparing across categories, we see that exchanges account for a considerable fraction of the total value of these users. More surprisingly, given the payout-based nature of mining pools, Figure 5a also seems to indicate that mining pools are receiving a large portion of incoming value. This percentage is artificially inflated, however, by certain artifacts of how mining pools, and Deepbit in particular, pay their miners. In fact, as we see in Figure 5b, over 80% of the value Deepbit receives is as change from itself.

While the particular mechanism that Deepbit uses allows us to eliminate this "self-churn" even using Heuristic 1 (as they always use a self-change address), more generally we cannot eliminate the self-churn of all users with just Heuristic 1. We are able to identify self-churn only if we know that the change address is controlled by the same user as the input address(es).

Eliminating this self-churn is therefore where Heuristic 2 becomes crucial. To see the effect it has, we compare the self-churn of Mt. Gox as determined using the two heuristics. Figure 5c shows that finding additional change addresses for Mt. Gox using Heuristic 2 essentially doubles the estimate of churn activity of Mt. Gox compared to using Heuristic 1 (and we observed a similar doubling when considering the churn in bitcoin value rather than activity).

[4]This usage is quite common: 23% of all transactions in the past six months are self-change transactions. For example, it is the standard option for the popular wallet service My Wallet, hosted by `blockchain.info`, as well as the way the Deepbit mining pool does its payouts.

4.5 Refining Heuristic 2

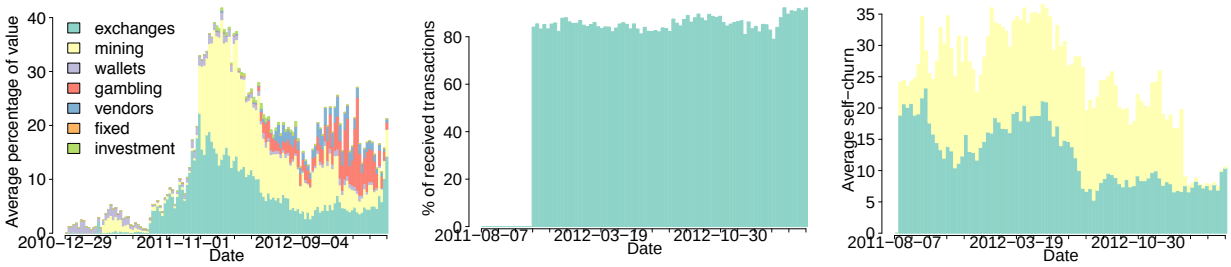
Although effective, Heuristic 2 is more challenging and significantly less safe than Heuristic 1. In our first attempt, when we used it as defined above, we identified over 4 million change addresses. Due to our concern over its safety, we sought to approximate the false positive rate. To do this even in the absence of significant ground truth data, we used the fact that we could observe the behavior of addresses over time: if an address and transaction met the conditions of Definition 4.3 at one point in time (where time was measured by block height), and then at a later time the address was used again, we considered this a false positive. Stepping through time in this manner allowed us to identify 555,348 false positives, or 13% of all labeled change accounts.

We then considered ways of making the heuristic more conservative. First, however, a manual inspection of some of these false positives revealed an interesting pattern: many of them were associated with transactions to and from Satoshi Dice and other dice games. By looking further into the payout structure of these games, it became clear that these were not truly false positives, as when coins are sent to Satoshi Dice, the payout is sent back to the same address. If a user therefore spent the contents of a one-time change address with Satoshi Dice, the address would receive another input back from Satoshi Dice, which would appear to invalidate the "one-timeness" of the address. We therefore chose to ignore this case, believing that addresses that received later inputs solely from Satoshi Dice could still be one-time change addresses. By doing so the false positive rate reduces to only 1%. We next considered waiting to label an address as a change address; i.e., waiting to see if it received another input. Waiting a day drove the false positive rate down to 0.28%; waiting a week drove it down to 0.17%, or only 7,382 false positives total.

Despite all these precautions, when we clustered users using this modified heuristic, we still ended up with a giant super-cluster containing the public keys of Mt. Gox, Instawallet, BitPay, and Silk Road, among others; in total, this super-cluster contained 1.6 million public keys. After a manual inspection of some of the links that led to this super-cluster, we discovered two problematic patterns. First, especially within a short window of time, the same change address was sometimes used twice. If this change address were then used the second time with a new address, the new address would appear to be the change address and be falsely labeled as such. Second, certain addresses would occasionally be used as "self-change" addresses (recall the second requirement in Definition 4.3), and then later used as separate change addresses; again, if the time they were used separately was with a new address, the new address would be falsely labeled as the change address. This behavior is likely due to the advanced features in some wallets, such as My Wallet and the desktop client Armory, that allow users to explicitly specify the change address for a transaction.

We thus further refined our heuristic by ignoring transactions involved with either of these types of behavior. For transactions in which an output had already received only one input, or for transactions in which an output had been previously used in a self-change transaction, we chose to not tag anything as the change address. Doing so, and manually removing a handful of other false positives (with no discernible pattern), we identified 3,540,831 change addresses.

Using this refined Heuristic 2 produces 3,384,179 clusters, which we were able to again collapse slightly (using our tags) to 3,383,904 distinct clusters. Of these clusters, we were able to name 2,197 of them (accounting for over 1.8 million addresses); although this might seem like a small fraction, recall that by participating in 344 transactions we hand-tagged only 1,070 addresses, and thus Heuris-



(a) The incoming value over time, as a percentage of total weekly incoming value, for each of the major categories. The teal and yellow categories are exchanges and mining pools respectively.

(b) Of transactions sent to Deepbit, the percentage that were sent by Deepbit itself (i.e., the percentage that was self-churn). The transactions from Deepbit account for over 80% of its incoming transactions.

(c) The percentage of all transactions received by Mt Gox that were sent by Mt Gox. The teal shows self-churn identified by Heuristic 1; the yellow shows *additional* churn identified by Heuristic 2.

Figure 5: Figures illustrating the effect of self-churn on measurements, and the different ways Heuristics 1 and 2 deal with self-churn.

tic 2 allowed us to name 1,600 times more addresses than our own manual observation provided. Furthermore, as we see in the visualization of the user graph depicted in Figure 6, and will argue in Section 5, the users we were able to name capture an important and active slice of the Bitcoin network.

Having finally convinced ourselves of both the safety of Heuristic 2, by refining it substantially, and its effectiveness, as illustrated in Figure 5c, we use Heuristic 2 exclusively for the results in the next section.

5. SERVICE CENTRALITY

In this section, we focus on two notable parts of the user graph seen in Figure 6: the component consisting of Satoshi Dice and the individuals who interact with it, and the heavily connected component consisting of most of the services we tagged. For both of these components, we argue that the demonstrated centrality of these services makes it difficult for even highly motivated individuals — e.g., thieves or others attracted to the anonymity properties of Bitcoin — to stay completely anonymous, provided they are interested in cashing out by converting to fiat money (or even other virtual currencies).

5.1 The effect of popular services

One of the largest stresses on the Bitcoin system to date has been the introduction of so-called dice games, and in particular Satoshi Dice, a betting game introduced in late April 2012. Briefly, users may place bets with various addresses, each of which is associated with a probability of winning (ranging from a 0.0015% chance of winning to a 97% chance). After determining if the user has won (using an algorithm involving the bet transaction and a random number), Satoshi Dice then sends some multiplier of the user's bet back to him if he won (e.g., 1.004 times his bet if he sent to the address with 97% winning odds), and 1 satoshi (0.00000001 BTC) if he lost.

Within weeks of being introduced, Satoshi Dice became wildly popular. Figure 7a shows its activity as compared to the activity of the Deepbit mining pool, which was arguably the most active user prior to the introduction of dice games. Satoshi Dice engages in tens of thousands of transactions per day, or about 60% of the overall activity in the Bitcoin network. It has also spawned a number of clones, such as BTC Dice, BTCLucky, Clone Dice, and DiceOnCrack (which, although less popular, are nevertheless quite well connected, as seen in Figure 6).

A number of factors help explain the popularity of Satoshi Dice. First, it allows users to place very small bets: the minimum bet for each category is 0.01 BTC, and over 21% of all bets (896,864 out of 4,127,979) are exactly this minimum value. Figure 7b shows that Satoshi Dice — just in terms of its outgoing transactions — accounts for anywhere between 30% and 40% of such micro-valued transactions (we found very similar results looking instead at the incoming transactions for Satoshi Dice). Referring back to Figure 2 and the rise of micro-valued transactions, we conclude that a large fraction of this rise can be attributed just to Satoshi Dice. In addition to allowing small bets, Satoshi Dice also acts extremely quickly. Once a bet is placed, the outcome is decided immediately and the payout is returned within seconds, as shown in Figure 7c. As with micro-valued transactions, referring back to Figure 3 indicates that Satoshi Dice also accounts for much of the rise of immediate spending (as a weekly average, nearly 50% of immediate transactions are due to Satoshi Dice).

Because of its immense popularity, and the extent to which it has inflated the size of the block chain (an extra 30,000 transactions translates into an extra 14MB added to the overall block chain daily), the opinion of Satoshi Dice in the Bitcoin community is somewhat mixed: some decry it as a DoS attack,[5] while others appreciate that it has stress-tested the Bitcoin network.

It might be tempting to additionally think that, given the large amounts of bitcoins flowing through it, Satoshi Dice could act as a mix service:[6] if "dirty" bitcoins were gambled using 97% winning odds, and the resulting bitcoins were paid out to a different address, these bitcoins might at first glance appear to have no association with the gambled money (especially if they came from a different address than the gambled money was sent to, as is sometimes the case). Because the addresses that Satoshi Dice uses are public, however, it is trivial to observe when users are gambling; furthermore, in sending a bet to Satoshi Dice, a user must explicitly identify where the payout should be sent. Thus, without using services such as Satoshi Dice as a co-conspirator (which they seem to have no incentive to do, as they made over $500,000 in their first eight months alone [11]), the bitcoins paid out are indelibly linked to the ones that were placed as a bet.

5.2 Traffic analysis of illicit activity

We next turn our attention to another dominant category of service: exchanges. Although not nearly as active as Satoshi Dice, exchanges have essentially become chokepoints in the Bitcoin econ-

[5] `http://en.bitcoin.it/wiki/SatoshiDice`

[6] See, for example, early concerns at `bitcointalk.org/index.php?topic=79079.0` and related discussions.

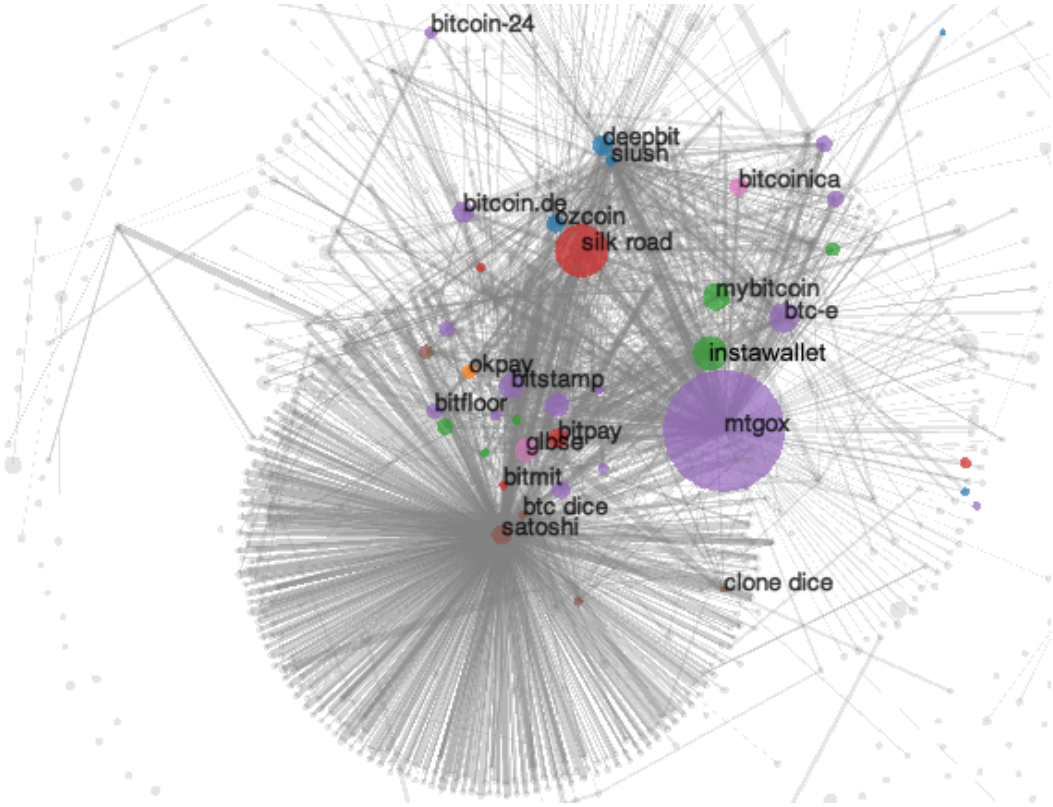


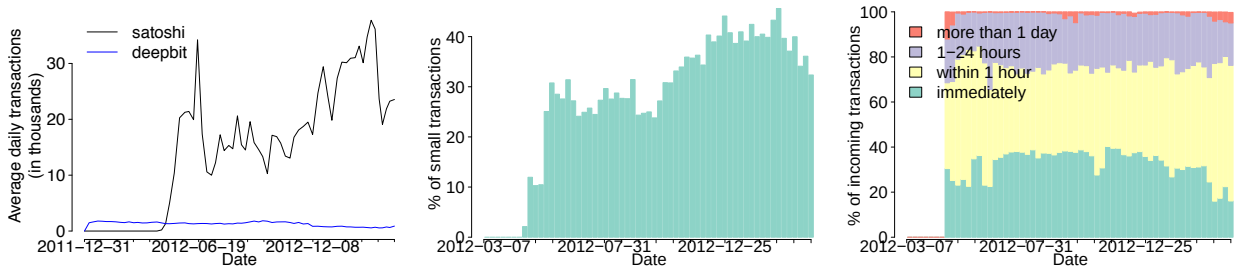
Figure 6: A visualization of the user network. The area of the cluster represents the external incoming value; i.e., the bitcoins received from other clusters but not itself, and for an edge to appear between two nodes there must have been at least 200 transactions between them. The nodes are colored by category: blue nodes are mining pools; orange are fixed-rate exchanges; green are wallets; red are vendors; purple are (bank) exchanges; brown are gambling; pink are investment schemes; and grey are uncategorized.

omy: to buy into or cash out of Bitcoin at scale, we argue that using an exchange is unavoidable. While sites like `localbitcoins.com` and `bitcoinary.com` do allow you to avoid exchanges (for the former, by matching up buyers directly with sellers in their geographic area), the current and historical volume on these sites does not seem to be high enough to support cashing out *at scale*.

For criminals, this centrality presents a unique problem: if a thief steals thousands of bitcoins, this theft is unavoidably visible within the Bitcoin network, and thus the initial address of the thief is known and (as most exchanges try to maintain some air of reputability) he cannot simply transfer the bitcoins directly from the theft to a known exchange.[7] While he might attempt to use a mix service to hide the source of the money, we again argue that these services do not currently have the volume to launder thousands of bitcoins. As such, thieves have developed various strategies for hiding the source of the bitcoins that we explore in this section. In particular, we focus on the effectiveness of Heuristic 2 in deanonymizing these flows, and thus in tracking illicitly-obtained bitcoins to exchanges (and thus, e.g., providing an agency with subpoena power the opportunity to learn whose account was deposited into, and in turn potentially the identity of the thief). For this approach to work, we do not need to (and cannot) account for each and every stolen bitcoin, but rather need to demonstrate only some flow of bitcoins directly from the theft to an exchange or other known institution.

To demonstrate the effectiveness of Heuristic 2 in this endeavor, we focus on an idiom of use that we call a "peeling chain." The usage of this pattern extends well beyond criminal activity, and is seen (for example) in the withdrawals for many banks and exchanges, as well as in the payouts for some of the larger mining pools. In a peeling chain, a single address begins with a relatively large amount of bitcoins (e.g., for mining pools it starts with the 25 BTC reward). A smaller amount is then "peeled" off this larger amount, creating a transaction in which a small amount is transferred to one address (e.g., 0.1 BTC for a miner payout), and the remainder is transferred to a one-time change address. This process is repeated — potentially for hundreds or thousands of hops — until the larger amount is pared down, at which point (in one usage) the amount remaining in the address might be aggregated with other such addresses to again yield a large amount in a single address, and the peeling process begins again. By using Heuristic 2, we are able to track flows of money by following these change links systematically: at each hop, we look at the two output addresses in the transaction. If one of these outputs is a change address, we can follow the chain to the next hop by following the change address (i.e., the next hop is the transaction in which this change address spends its bitcoins), and can identify the meaningful recipient in the transaction as the other output address (the "peel").

[7] Indeed, the Bitcoin community has recently demonstrated both the inherent traceability of thefts and the unwillingness to accept stolen money (see `bitcointalk.org/index.php?topic=14085.msg1910231`). After 923 BTC was stolen from the mining pool Ozcoin and transferred to a Strongcoin wallet, Strongcoin intercepted the bitcoins when the thief attempted to withdraw them and returned them to Ozcoin.



(a) The overall daily activity, in terms of number of both incoming and outgoing transactions, for Satoshi Dice, as compared to the overall activity for the mining pool Deepbit.

(b) The percentage of transactions with less than 0.1 BTC in total value in which Satoshi Dice participated as the sender, shown as an average weekly percentage.

(c) A breakdown of how quickly Satoshi Dice spends the money it receives: teal is immediately, yellow is within an hour, purple is within a day, and red is more than a day.

Figure 7: The effect Satoshi Dice has had on the Bitcoin network, in terms of both activity and its influence on trends.

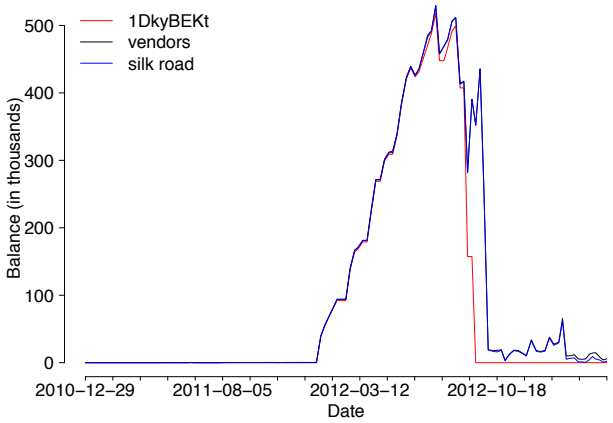


Figure 8: The balance of the vendors category (in black, although barely visible because it is dominated by Silk Road), Silk Road (in blue), and the `1DkyBEKt` address (in red).

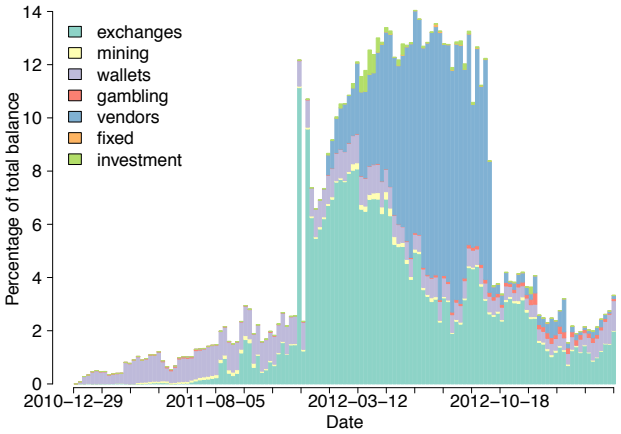


Figure 9: The balance of each major category, represented as a percentage of total active bitcoins; i.e., the bitcoins that are not held in sink addresses.

Silk Road and Bitcoin Savings & Trust.

One of the most well-known and heavily scrutinized addresses in Bitcoin's history is `1DkyBEKt`,[8] which is believed to be associated with Silk Road and was active between January and September 2012. Starting in January, the address began to receive large aggregate sums of bitcoins; in the first of these, the funds of 128 addresses were combined to deposit 10,000 BTC into the `1DkyBEKt` address, and many transactions of this type followed (including one transaction in which the funds of 589 addresses were combined to deposit 8,000 BTC). All together, the address received 613,326 BTC in a period of eight months, receiving its last aggregate deposit on August 16 2012.

Then, starting in August 2012, bitcoins were aggregated and withdrawn from `1DkyBEKt`: first, amounts of 20,000, 19,000, and 60,000 BTC were aggregated and sent to separate addresses; later, 100,000 BTC each was sent to two distinct addresses, 150,000 BTC to a third, and 158,336 BTC to a fourth, effectively emptying the `1DkyBEKt` address of all of its funds. The balance of this address over time, as well as the balance of Silk Road and of vendors as a whole (as we consider Silk Road a vendor), is shown in Figure 8.

Due to its large balance (at its height, it contained 5% of all generated bitcoins), as well as the curious nature of its rapidly accumulated wealth and later dissolution, this address has naturally been the subject of heavy scrutiny by the Bitcoin community. While it is largely agreed that the address is associated with Silk Road (and indeed our clustering heuristic did tag this address as being controlled by Silk Road), some have theorized that it was the "hot" (i.e., active) wallet for Silk Road, and that its dissipation represents a changing storage structure for the service. Others, meanwhile, have argued that it was the address belonging to the user pirate@40, who was responsible for carrying out the largest Ponzi scheme in Bitcoin history (the investment scheme Bitcoin Savings & Trust, which is now the subject of a lawsuit brought by the SEC [20]).

To see where the funds from this address went, and if they ended up with any known services, we first plotted the balance of each of the major categories of services, as seen in Figure 9. Looking at this figure, it is clear that when the address was dissipated, the resulting funds were not sent en masse to any major services, as the balances of the other categories do not change significantly. To nevertheless attempt to find out where the funds did go, we turn to the traffic analysis described above.

In particular, we focus on the last activity of the `1DkyBEKt` address, when it deposited 158,336 BTC into a single address. This address then peeled off 50,000 BTC each to two separate addresses, leaving 58,336 BTC for a third address; each of these addresses then began a peeling chain, which we followed using the methodology described above (i.e., at each hop we continued along the chain by following the change address, and considered the other output

[8] Full address: `1DkyBEKt5S2GDtv7aQw6rQepAvnsRyHoYM`.

	First		Second		Third	
Service	Peels	BTC	Peels	BTC	Peels	BTC
Bitcoin-24			1	2	3	124
Bitcoin Central					2	2
Bitcoin.de					1	4
Bitmarket					1	1
Bitstamp			5	97	1	1
BTC-e					1	250
CA VirtEx	1	3	1	10	3	22
Mercado Bitcoin					1	9
Mt. Gox	11	492	14	70	5	35
OKPay	2	151			1	125
Instawallet	7	39	5	135	2	43
WalletBit	1	1				
Bitzino					2	1
Seals with Clubs	1	8				
Coinabul			1	29		
Medsforbitcoin	3	10				
Silk Road	4	28			5	102

Table 2: Tracking bitcoins from `1DkyBEKt`. Along the first 100 hops of the first, second, and third peeling chains resulting from the withdrawal of 158,336 BTC, we consider the number of peels seen to each service, as well as the total number of bitcoins (rounded to the nearest integer value) sent in these peels. The services are separated into the categories of exchanges, wallets, gambling, and vendors.

address to be a meaningful recipient of the money). After following 100 hops along each chain, we observed peels to the services listed in Table 2.

Looking at this table, we see that, although a longitudinal look at the balances of major services did not reveal where the money went, following these chains revealed that bitcoins were in fact sent to a variety of services. The overall balance was not highly affected, however, as the amounts sent were relatively small and spread out over a handful of transactions. Furthermore, while our analysis does not itself reveal the owner of `1DkyBEKt`, the flow of bitcoins from this address to known services demonstrates the prevalence of these services (54 out of 300 peels went to exchanges alone) and provides the potential for further de-anonymization: the evidence that the deposited bitcoins were the direct result of either a Ponzi scheme or the sale of drugs might motivate Mt. Gox or any exchange (e.g., in response to a subpoena) to reveal the account owner corresponding to the deposit address in the peel, and thus provide information to link the address to a real-world user.

Tracking thefts.

To ensure that our analysis could be applied more generally, we turned finally to a broader class of criminal activity in the Bitcoin network: thefts. Thefts are in fact quite common within Bitcoin: almost every major service has been hacked and had bitcoins (or, in the case of exchanges, other currencies) stolen, and some have shut down as a result.

To begin, we used a list of major Bitcoin thefts;[9] some of the thefts did not have public transactions (i.e., ones we could identify and study in the block chain), so we limited our attention to

[9] `https://bitcointalk.org/index.php?topic=83794.0`

Theft	BTC	Date	Movement	Exchanges?
MyBitcoin	4019	Jun 2011	A/P/S	Yes
Linode	46,648	Mar 2012	A/P/F	Yes
Betcoin	3171	Mar 2012	F/A/P	Yes
Bitcoinica	18,547	May 2012	P/A	Yes
Bitcoinica	40,000	Jul 2012	P/A/S	Yes
Bitfloor	24,078	Sep 2012	P/A/P	Yes
Trojan	3257	Oct 2012	F/A	No

Table 3: Tracking thefts. For each theft, we list (approximately) how many bitcoins were stolen, when the theft occurred, how the money moved after it was stolen, and whether we saw any bitcoins sent to known exchanges. For the movement, we use A to mean aggregation, P to mean a peeling chain, S to mean a split, and F to mean folding, and list the various movements in the order they occurred.

the ones that did. For each theft, we first found the specific set of transactions that represented the theft; i.e., the set of transactions in which the sender was the service being stolen from, and the recipient was the thief. Starting with these transactions, we did a preliminary manual inspection of the transactions that followed to determine their approximate type: we considered aggregations, in which bitcoins were moved from several addresses into a single one; folding, in which some of the addresses involved in the aggregation were not clearly associated with the theft, and thus were potentially there to "clean" the stolen money; splits, in which a large amount of bitcoins was split among two or more addresses; and finally peeling chains, in which relatively small amounts were peeled off from a succession of one-time change addresses holding a large amount of bitcoins. Our results are summarized in Table 3.

Briefly, the movement of the stolen money ranged from quite sophisticated layering and mixing to simple and easy to follow. Examining thefts therefore provides another demonstration of the potential for anonymity provided by Bitcoin, and the ways in which current usage falls short of this potential: for the thieves who used the more complex strategies, we saw little opportunity to track the flow of bitcoins (or at least do so with any confidence that ownership was staying the same), but for the thieves that did not there seemed to be ample opportunity to track the stolen money directly to an exchange.

One of the easiest thefts to track was from Betcoin, an early gambling site that was shut down after its server was hacked on April 11 2012 and 3,171 BTC were stolen in four installments of 2,902, 165, 17, and 87 BTC each. The stolen bitcoins then sat in the thief's address until March 15 2013 (when the bitcoin exchange rate began soaring), when they were aggregated with other small addresses into one large address that then began a peeling chain. After 10 hops, we saw a peel go to Bitcoin-24, and in another 10 hops we saw a peel go to Mt. Gox; in total, we saw 374.49 BTC go to known exchanges, all directly off the main peeling chain, which originated directly from the addresses known to belong to the thief. For some of the other thefts, de-anonymizing the flow of bitcoins was similarly straightforward: for the May 2012 Bitcoinica theft, for example, we observed one peeling chain, occurring directly after an aggregation of addresses belonging to the thieves, in which large amounts (i.e., hundreds of bitcoins) were peeled off directly to known exchanges; in total, we saw 4,588 BTC peeled off to three different exchanges (BTC-e, CampBX, and Bitstamp). Again, although we do not account for every stolen bitcoin, watching even

a portion of them flow to exchanges provides the opportunity we need to potentially compromise the anonymity of the thieves.

In contrast, some of the other thieves used more sophisticated strategies to attempt to hide the flow of money; e.g., for the Bitfloor theft, we observed that large peels off several initial peeling chains were then aggregated, and the peeling process was repeated. Nevertheless, by manually following this peel-and-aggregate process to the point that the later peeling chains began, we systematically followed these later chains and again observed peels to multiple known exchanges: the third peel off one such chain was 191.09 BTC to Mt. Gox, and in total we saw 661.12 BTC sent to three popular exchanges (Mt. Gox, BTC-e, and Bitstamp).

Even the thief we had the most difficulty tracking, who stole bitcoins by installing a trojan on the computers of individual users, seemed to realize the difficulty of cashing out at scale. Although we were unable to confidently track the flow of the stolen money that moved, most of the stolen money did not in fact move at all: of the 3,257 BTC stolen to date, 2,857 BTC was still sitting in the thief's address, and has been since November 2012.

With these thefts, our ability to track the stolen money provides evidence that even the most motivated Bitcoin users (i.e., criminals) are engaging in idioms of use that allow us to erode their anonymity. While one might argue that thieves could easily thwart our analysis, as Heuristic 2 is admittedly not robust in the face of adversarial behavior, our observation is that — at least at present — none of the criminals we studied seem to have taken such precautions. We further argue that the fairly direct flow of bitcoins from the point of theft to the deposit with an exchange provides some evidence that using exchanges to cash out at scale is inevitable, and thus that — again, at present — Bitcoin does not provide a particularly easy or effective way to transact large volumes of illicitly-obtained money.

6. RELATED WORK

Since its inception, questions regarding the security — and in particular the anonymity — of Bitcoin have received considerable interest. On the first front, much work has concerned the strength of Bitcoin's settlement mechanism and the difficulty of an adversary in subverting it. The two best known explorations concerning Bitcoin "double spending" are from Karame et al. [9] and Meni Rosenfeld [19]. At their core, both focus on the tradeoffs between latency (the number of confirmations made through the Bitcoin network) and the computational requirements of an attacker — a tradeoff that implicitly explains the different risk regimes operational in the Bitcoin ecosystem today.

The second thrust of Bitcoin security research, closer to our own interest, has focused on the anonymity of its transactions. In 2011, fueled by the high-profile MyBitcoin theft, Reid and Harrigan [17] provided one of the first written analyses. Using a clustering algorithm similar to our Heuristic 1, they obtained a condensed "user" graph, and used it to describe the flow of stolen money from the aforementioned theft. In a more recent paper, Ron and Shamir [18] performed a similar analysis over the user graph (again using an heuristic similar to our Heuristic 1), and provided an in-depth examination of the largest transactions in Bitcoin history. From this data they conclude that there is massive hoarding in the Bitcoin system and that the vast majority of capital does not circulate. Concurrently with the work of Ron and Shamir, Androulaki et al. [2] applied a similar analysis, but focused more squarely on privacy concerns. Unlike Ron and Shamir, their analysis attempts to account for the complexity of "change" accounts which are central to how Bitcoin is used in practice. Applying this analysis to a *simulated* Bitcoin graph (in which ground truth data was known), 40% of user identities were correctly classified through such clustering. As we mention briefly in Section 4.3, their approach is insufficient for an empirical characterization of Bitcoin traffic since the assumptions it makes (particularly around the use of multi-output transactions) are routinely violated today. On the constructive side, Miers et al. [12] presented Zerocoin, a system designed to cryptographically amplify the anonymity guarantees in Bitcoin, precisely motivated by potential of the analysis techniques described in this paper.[10] Most recently, Möser [14] examined the anonymity of three Bitcoin mix services, and found that some were more successful than others, although all had a distinct transaction graph pattern due to their centralized nature.

Finally, we are aware of three analyses of key parts of the Bitcoin economy: Kroll et al.'s economic analysis of Bitcoin mining [10], Christin's study of the Silk Road marketplace [4] and Moore and Christin's analysis of Bitcoin exchange failures [13]. The first paper applies a game-theoretic analysis to the mining mechanism of Bitcoin, and in particular creates a formal model for a 51% (or "Goldfinger") attack, in which a cartel of miners are responsible for over half of the blocks being mined. They then discuss the circumstances under which such an attack could take place, and conclude that Bitcoin governance is not only inevitable but also necessary for the future of the currency. The second effort uses regular Web crawling of the Silk Road marketplace to characterize the popularity of illicit goods (typically controlled substances) and to estimate the total market value of such transactions. While this work does not examine the Bitcoin block chain at all, it could be used in tandem with our analysis to estimate the spread of such "dirty money" in the Bitcoin graph. Finally, the third paper is driven by the central role of Bitcoin exchanges, which are commonly used to deposit user funds. However, by escrowing funds with a third party outside the protections of the Bitcoin protocol, users can, and are, exposed to the risk of these exchanges failing. Moore and Christin provide a meta-analysis showing that almost half of all such exchanges have failed, and that failure is positively correlated to transaction volume (which they hypothesize is because the risk of a data breach is related to the value a criminal may obtain through such an action). While the authors do not focus on anonymity, we note that such breaches also provide large amounts of labeling data by which the broader Bitcoin graph can be de-anonymized.

7. CONCLUSIONS

In this study, we presented a longitudinal characterization of the Bitcoin network, focusing on the rise of services and the growing gap — due to certain idioms of use — between the potential anonymity available in the Bitcoin protocol design and the actual anonymity that is currently achieved by users. To accomplish this task, we developed a new clustering heuristic based on change addresses, allowing us to cluster addresses belonging to the same user. Then, using a small number of transactions labeled through our own empirical interactions with various services, we identify major institutions and the interactions between them. Even our relatively small experiment demonstrates that this approach can shed considerable light on the structure of the Bitcoin economy, how it is used, and those organizations who are party to it.

Although our work examines the current gap between actual and potential anonymity, one might naturally wonder — given that our new clustering heuristic is not fully robust in the face of chang-

[10]The authors write, "There is reason to believe that sophisticated results from other domains (e.g., efforts to deanonymize social network data using network topology) will soon be applied to the Bitcoin transaction graph."

ing behavior — how this gap will evolve over time, and what users can do to achieve stronger anonymity guarantees. We argue that to completely thwart our heuristics would require a significant effort on the part of the user, and that this loss of usability is unlikely to appeal to all but the most motivated users (such as criminals). Nevertheless, we leave a quantitative analysis of this hypothesis as an interesting open problem.

Acknowledgments

We would like to thank Brian Kantor and Cindy Moore for managing our systems and storage needs, and for helping to set up and maintain our mining rig. We are also grateful to Andreas Pitsillidis for his advice in creating figures and overall useful discussions. Finally, we thank our anonymous reviewers and our shepherd, Katerina Argyraki, for their helpful feedback and guidance.

This work was supported by National Science Foundation grants NSF-1237264 and NSF-1237076, by the Office of Naval Research MURI grant N00014-09-1-1081, and by generous research, operational and/or in-kind support from Google, Microsoft, Yahoo, and the UCSD Center for Networked Systems (CNS).

8. REFERENCES

[1] G. Andresen. bitcointools. github.com/gavinandresen/bitcointools.

[2] E. Androulaki, G. Karame, M. Roeschlin, T. Scherer, and S. Capkun. Evaluating User Privacy in Bitcoin. In *Proceedings of Financial Cryptography 2013*, 2013.

[3] CBC News. Revenue Canada says BitCoins aren't tax exempt, Apr. 2013. www.cbc.ca/news/canada/story/2013/04/26/business-bitcoin-tax.html.

[4] N. Christin. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. In *Proceedings of WWW 2013*, 2013.

[5] B. P. Eha. Get ready for a Bitcoin debit card. CNNMoney, Apr. 2012. money.cnn.com/2012/08/22/technology/startups/bitcoin-debit-card/index.html.

[6] European Central Bank. Virtual Currency Schemes. ECB Report, Oct. 2012. www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

[7] Federal Bureau of Investigation. (U) Bitcoin Virtual Currency Unique Features Present Distinct Challenges for Deterring Illicit Activity. Intelligence Assessment, Cyber Intelligence and Criminal Intelligence Section, Apr. 2012. cryptome.org/2012/05/fbi-bitcoin.pdf.

[8] FinCEN. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, Mar. 2013. www.fincen.gov/statutes_regs/guidance/pdf/FIN-2013-G001.pdf.

[9] G. Karame, E. Androulaki, and S. Capkun. Double-Spending Fast Payments in Bitcoin. In *Proceedings of ACM CCS 2012*, 2012.

[10] J. A. Kroll, I. C. Davey, and E. W. Felten. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. In *Proceedings of WEIS 2013*, 2013.

[11] J. Matonis. Bitcoin Casinos Release 2012 Earnings. Forbes, Jan. 2013. www.forbes.com/sites/jonmatonis/2013/01/22/bitcoin-casinos-release-2012-earnings/.

[12] I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous Distributed E-Cash from Bitcoin. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2013.

[13] T. Moore and N. Christin. Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk. In *Proceedings of Financial Cryptography 2013*, 2013.

[14] M. Möser. Anonymity of Bitcoin Transactions: An Analysis of Mixing Services. In *Proceedings of Münster Bitcoin Conference*, 2013.

[15] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System, 2008. bitcoin.org/bitcoin.pdf.

[16] M. Peck. Bitcoin-Central is Now The World's First Bitcoin Bank...Kind Of. IEEE Spectrum: Tech Talk, Dec. 2012. spectrum.ieee.org/tech-talk/telecom/internet/bitcoincentral-is-now-the-worlds-first-bitcoin-bankkind-of.

[17] F. Reid and M. Harrigan. An Analysis of Anonymity in the Bitcoin System. In *Security and Privacy in Social Networks*, pages 197–223. Springer New York, 2013.

[18] D. Ron and A. Shamir. Quantitative Analysis of the Full Bitcoin Transaction Graph. In *Proceedings of Financial Cryptography 2013*, 2013.

[19] M. Rosenfeld. Analysis of hashrate-based double-spending, Dec. 2012. bitcoil.co.il/Doublespend.pdf.

[20] Securities and Exchange Commission. SEC Charges Texas Man With Running Bitcoin-Denominated Ponzi Scheme, July 2013. www.sec.gov/News/PressRelease/Detail/PressRelease/1370539730583.

[21] znort987. blockparser. github.com/znort987/blockparser.