

How Did Dread Pirate Roberts Acquire and Protect His Bitcoin Wealth?

Dorit Ron and Adi Shamir

Department of Computer Science and Applied Mathematics,
The Weizmann Institute of Science, Israel
{dorit.ron, adi.shamir}@weizmann.ac.il

Abstract. The Bitcoin scheme is one of the most popular and talked about alternative payment schemes. It was conceived in 2008 by the mysterious Satoshi Nakamoto, whose real identity remains unknown even though his bitcoin holdings are believed to be worth several hundred million dollars. One of the most active parts of the Bitcoin ecosystem was the Silk Road marketplace, in which highly illegal substances and services were traded. It was run by another mysterious person who called himself Dread Pirate Roberts (DPR), whose bitcoin holdings are also estimated to be worth hundreds of millions of dollars at today's exchange rate. On October 1-st 2013, the FBI arrested a 29 year old person named Ross William Ulbricht, claiming that he is DPR, and seizing a small fraction of his bitcoin wealth. In this paper we use the publicly available record to trace the evolution of his holdings in order to find how he acquired and how he tried to hide them from the authorities. For example, we show that all his income from the months of May, June and September 2013, along with numerous other amounts, were not seized by the FBI. One of the most surprising discoveries we made during our analysis was the existence of a recent substantial transfer (which was worth more than 60,000 dollars when made on March 20-th 2013, and close to a million dollars at today's exchange rate) which may link these two mysterious figures.

Keywords: Bitcoin, Silk Road, Dread Pirate Roberts, DPR, Satoshi Nakamoto

1 Introduction

Silk Road was an online marketplace which provided infrastructure for sellers and buyers to trade over the internet. In this sense it was similar to eBay, but with two major differences: most of the items offered for sale were illegal, and there was great emphasis on trying to ensure, as much as possible, the anonymity of both sellers and buyers. In particular, all the communication with the website was carried out through TOR ("The Onion Router"), in order to conceal the true IP addresses and therefore the identities of the network's users.

The Silk Road website was visited by hundreds of thousands of unique users from countries across the globe (about 30 percent of whom indicated upon registration that they were from the United States) [1]. It grew rapidly, and in

September 2013 had nearly 13,000 listings of drugs such as Cannabis, Ecstasy, etc. In addition, it offered a variety of services such as computer-hacking and items such as forged passports.

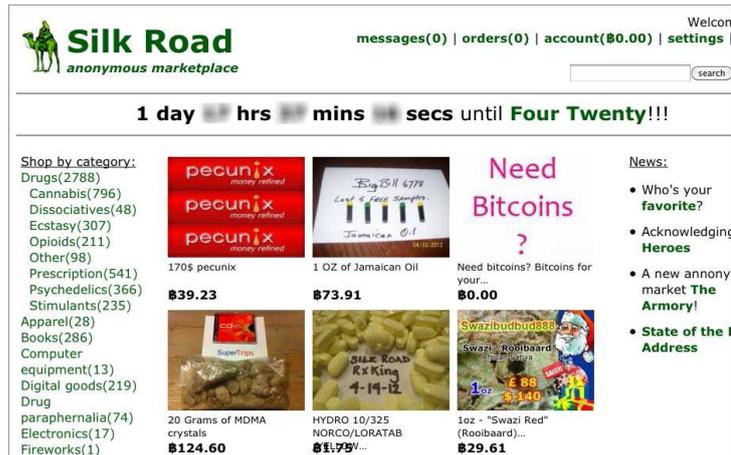
The only form of payment accepted on Silk Road was bitcoins. This is a decentralized form of electronic currency invented in 2008 by Satoshi Nakamoto [2], whose real identity remains a major mystery. In this scheme, all the transactions of all the users are publicly available (for instance via the so called block explorer [3]) but in an anonymous way [4]. Silk Road’s payment system essentially consisted of an internal bitcoin “bank”, where every Silk Road user had to hold at least one account in order to conduct transactions on the site. These accounts were stored on wallets maintained on servers controlled by Silk Road. Each user had to deposit bitcoins in advance into his Silk Road account, and then he was free to use them in order to buy multiple items on Silk Road. When a purchase was made, the appropriate number of bitcoins was first transferred to an escrow account maintained by Silk Road, pending completion of the transaction. When the transaction was completed, the buyers’ bitcoins were transferred from the escrow account to the Silk Road bitcoin address of the vendor involved in the sale. Silk Road also used a so-called “tumbler” which, as the site explained, “sent all payments through a complex, semi-random series of dummy transactions making it nearly impossible to link your payment with any coins leaving the site” [1].

The paper is organized as follows. Section 2 describes what is known about the alleged owner and operator of the Silk Road marketplace website. In section 3 we trace backwards all the accounts and amounts which are related to those which were seized by the FBI when they arrested Ulbricht and confiscated his computer, in order to better understand his financial activity and mode of operation. Finally, in Section 4 we describe a surprisingly short path involving substantial sums connecting DPR and a very early bitcoin account, which was created by one of the founders of the Bitcoin scheme (probably Satoshi Nakamoto himself).

2 Who Operated the Silk Road Marketplace?

The Silk Road marketplace opened in February 2011, and throughout its existence was operated by an unknown person who called himself Dread Pirate Roberts (DPR), who controlled every aspect of its operation: He acquired the computer infrastructure, maintained the Silk Road website, and determined vendor and customer policies (including deciding what can be sold on the site). He was paid a commission for each transaction, which varied depending on the size of the transaction: 10% for the first \$50 down to 1.5% for purchases over \$1000 [5]. On October 1-st 2013 the FBI arrested in San Francisco an American citizen named Ross William Ulbricht, claimed that he is DPR, and seized control of the Silk Road website (see Figure 1). As expected, a different website calling itself “The New Silk Road” was opened on November 6, 2013 [6], offering a similar collection of illegal items for sale (see Figure 2).

The old site of the Silk Road



Seized by the FBI on October 1th 2013



Fig. 1. The Silk Road's front page [5] and the seized FBI's announcement.

Reopened on November 6th 2013



The selection on the new Silk Road

Silk Road
anonymous market

messages 0 | orders 0 | account \$0.00

Search Go HL settings - logout

browsing drugs

item	vendor	price	
 1g DMT Freebase	ringo deathstarr	\$0.35672880	add to cart
 7g (14oz) PCubensis Powder	magjctd	\$0.16030500	add to cart
 FREE 25-NBOMe 1mg blotter sample FREE	eternaipsey	\$0.00000000	add to cart

- Drugs 227
 - Cannabis 24
 - Dissociatives 4
 - Ecstasy 30
 - Opioids 5
 - Other 15
 - Precursors 1
 - Prescription 39
 - Psychodelics 54
 - Stimulants 17
- Apparel 18
- Art 0
- Biatic materials 0
- Books 11
- Collectibles 0
- Computer equipment 2
- Custom Orders 0
- Digital goods 3
- Drug paraphernalia 5
- Electronics 0
- Erotica 0
- Forgeries 16
- Hardware 0
- Herbs & Supplements 0
- Jewelry 0
- Lab Supplies 1
- Lotteries & games 5
- Medical 0
- Money 3

Fig. 2. A message from the administrator of the new Silk Road announcing the re-opening of the new site and its new front page [7].

According to a press release from the United States attorney’s office [1], Silk Road was used during its two and a half year existence by several thousand drug dealers to distribute hundreds of kilograms of illegal drugs, to supply unlawful services to more than a hundred thousand buyers, and to launder hundreds of millions of dollars derived from these transactions. The site generated sales revenue of more than 9.5 million bitcoins and collected commissions from these sales totaling more than 600,000 bitcoins. At the bitcoin exchange rate in effect when the Silk Road website was seized, these figures are roughly equivalent to \$1.2 billion in sales and \$80 million in commissions. At today’s exchange rate, DPR’s wealth is estimated to be several hundred million dollars, and only a small fraction of this amount was seized so far by the FBI.

Table 1. Bitcoins received by DPR over time

Date	Amount	# of incoming transactions	# of small amounts	# of medium amounts	How much was seized	How much was moved	
10/12	12,564	2	-	540	-	5,502	7,062
11/12	42,263	6	-	1,596	-	12,463	29,800
12/12	5,275	-	1	-	50	0	5,275
1/13	63,000	5	3	2,580	71	41,350	21,650
2/13	6,000	2	-	586	-	2,650	3,350
3/13	44,642	1	3	466	66	43,442	1,200
4/13	5,000	-	-	-	6	3,550	1,450
5/13	0	-	-	-	-	0	0
6/13	0	-	-	-	-	0	0
7/13	27,018	2862	3	8586	34	27,018	0
8/13	8,361	2	1	244	4	8,361	0
9/13	0	-	-	-	-	0	0
	214,123					144,336	69,787

3 Tracing Backwards the Published Account

At the time of his arrest on October 1-st 2013, Ulbricht was using a laptop computer, which was seized by the FBI. Through forensic analysis which lasted 25 days, federal law enforcement agents found on this laptop a bitcoin wallet containing approximately 144,336 bitcoins [1]. Immediately afterwards, on October 25-th between 01:27:54 to 06:50:27, the FBI transferred the full amount (worth about \$28 million) in a series of 446 transactions to a single new account that they created and controlled. Each one of the first 445 transactions transferred exactly 324 BTCs (which is the numeric equivalent of “FBI” on a phone’s keypad), and the last one transferred the remaining 156 BTCs, as described in Figure 4. On the same day, they published the identity of the new account [8] which contained all the seized bitcoins, but even if they had refrained from doing so, the public nature of the Bitcoin scheme and the highly unusual series of

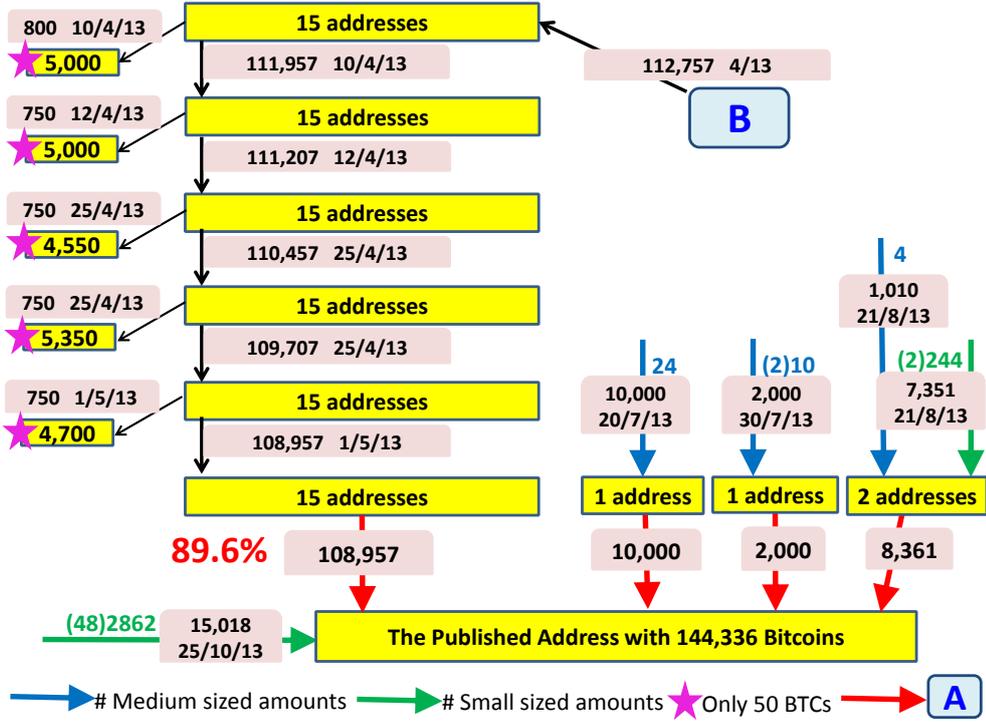


Fig. 3. The backtracking of the published address (at the bottom). 89.6% of the entire seized amount originated from only 19 addresses shown above the published address and connected to it by four red arrows, explained in Figure 4. The remaining 10.4% was seized from 2,862 small accounts grouped into 48 transactions as shown in green to the left of the published address. In the (x)y notation on the arrows, x indicates the number of involved transactions and y indicates the number (not the sum!) of the transferred amounts. The sum and the associated date of the transfer are written on the arrow. If there is just one transaction with y “from” accounts, (x) is omitted. Green arrows are associated with multiple small amounts of less than 60 BTCs and blue arrows are associated with multiple medium amounts of less than 1,000 BTCs.

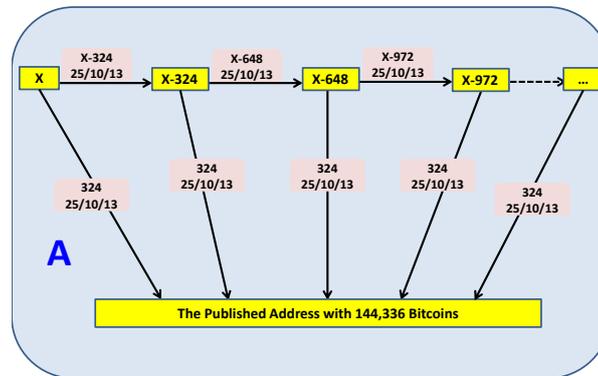


Fig. 4. Each red arrow in Figure 3 represents a large number of bitcoins found on DPR’s computer. It was seized by transferring it into an FBI-controlled account via a sequence of transactions, each moving exactly 324 bitcoins (except in the last transaction). Starting from the top-left with X bitcoins in a DPR-controlled account, 324 were seized and the remaining X-324 were moved to an intermediate address from which again 324 were seized, etc., until the entire amount was seized. All these transactions took place on 25/10/13 between 01:27:54 and 06:50:27.

identical transactions would have revealed its identity in any case. In the block explorer this address is titled “DPR Seized Coins”.

An interesting comment we would like to make is that the notion of seizing bitcoins from a suspect’s laptop is much trickier than the notion of seizing cash from a suspect’s safe, even if all the necessary keys are found by the FBI in both cases. In the case of cash, once the money is hauled away, it is no longer available to the suspect. However, let us assume that the Bitcoin community had noticed the unusual activity, and had refused to pick up these FBI-initiated transactions for verification as part of the official block chain. In this case, it would not help the FBI that they set up the new account and had initiated those transfers - their holdings would not be recognized as valid, and thus they would not be able to exchange or auction them off. In addition, they could still be used by either the suspect or by any one of his accomplices who happens to know the secret key! Even if the community had been late in recognizing these events and some miners would have picked up those transactions in the meantime, a 51% majority of the computing power available to miners could have forked the block chain just before these transactions, and grown a longer side chain which would invalidate all the blocks that contain the FBI transactions. However, by now it is probably too difficult to take such measures, and the seized bitcoins are no longer usable by DPR.

Immediately after hearing about DPR’s arrest, we decided to use the publicly available transaction data in the block chain in order to understand and analyze

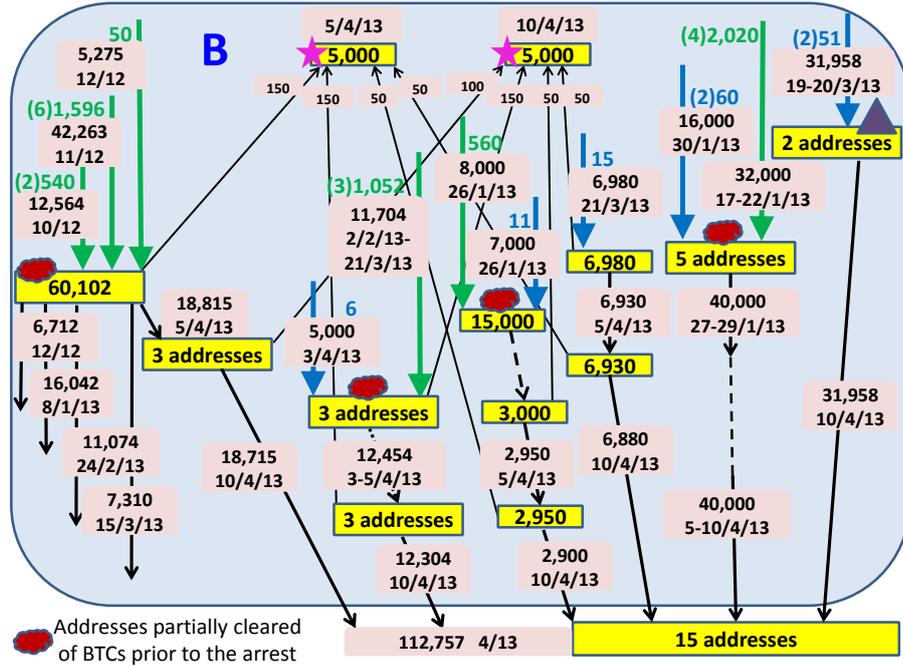


Fig. 5. Further backtracking of the largest accounts that the FBI claims to be owned by DPR reveals additional chunks of bitcoins that were there at some point, but were transferred elsewhere before October 1-st 2013 and thus were not seized. The sum of all these amounts is about 70,000 BTCs as listed in Table 1. Most of it was included in the four addresses marked with a brown cloud. The purple triangle on the top-right points to a very interesting address that we backtracked even further, as described in Figure 6.

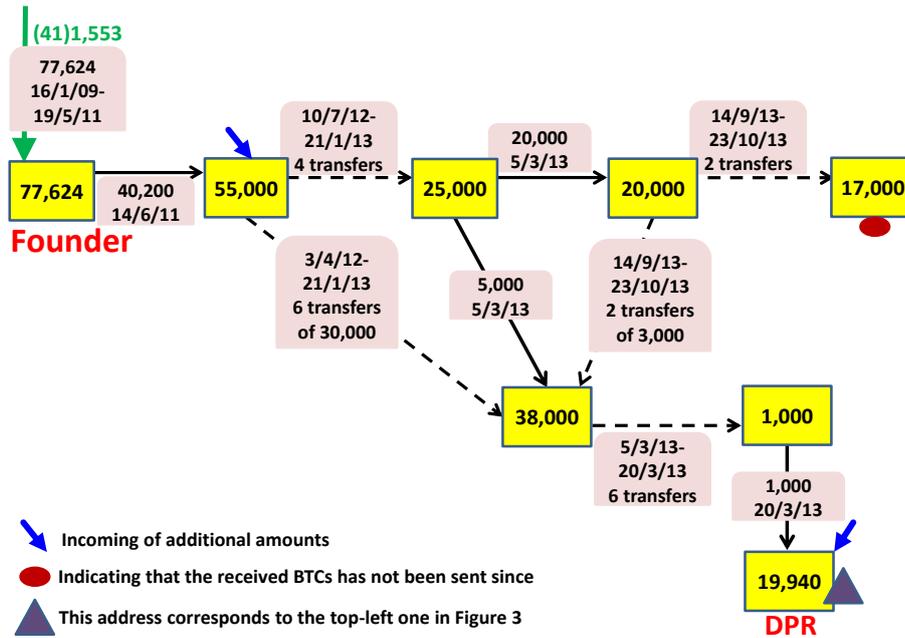


Fig. 6. Further backtracking of a single transfer of 1,000 BTCs (more than 60,000 dollars when made, and close to a million today) into the address marked by the purple triangle on the top-right of Figure 5, reveals its origin from an account which was created on January 16-th 2009, about one week after regular mining operations commenced in the Bitcoin system. We refer to the owner of this account as the **Founder** on the top-left of the figure. The 1,553 small amounts on the green arrow are mostly the result of mining operations, each yielding 50 BTCs.

DPR's mode of operation, and in particular how he acquired and how he tried to conceal his bitcoin wealth. Our starting point was the FBI-controlled account, and we tried to trace it backwards. Out of the 446 incoming transactions into the FBI account, 48 had many sending accounts, and the remaining 398 had between one and four sending accounts. Figure 3 summarizes the structure of the accounts which were the immediate predecessors of the FBI account. The FBI address is shown at the bottom of the figure. The five arrows entering it, one green and four red, represent its entire incoming flow of bitcoins. The green arrow indicates many transaction involving relatively *small* amounts of less than 60 BTCs each, and the notation along it indicates that a total of 15,018 bitcoins were transferred on October 25-th 2013 in 48 transactions with a total number of 2,862 "from" addresses included in all of them (the same notation will be used later on for the blue arrows, which represent *medium* sized transfers of between 60 and 1,000 BTCs). When there is only a single transaction, we omit the (1) from the label of the edge. The other 398 transactions backtracked to precisely 19 addresses which contained 89.6% of the 144,336 bitcoins which were seized from DPR's wallet. As described in Figure 3, DPR kept most of the bitcoins which were seized by the FBI in 15 accounts, and moved all his bitcoins simultaneously from one set of 15 accounts into another set of 15 accounts several times in April and May 2013, but then kept them in the same set of 15 accounts created on May 1-st 2013 until his arrest on October 1-st 2013. Each of these 15 addresses were used to send on the same dates exactly 50 bitcoins to certain accounts. On the left we show five such addresses marked by magenta asterisk, meaning that all its incoming transactions are exactly of 50 bitcoins. Backtracking some of these 50-bitcoin-transactions leads to several accounts which had hundreds of transactions with a huge total volume of hundreds of thousands of bitcoins. One of the largest among these accounts had more than 100,000 incoming BTCs and the last transaction in the account happened at 8AM on October 1-st 2013, just before DPR's arrest. It is not clear whether they belong to DPR, and none of these bitcoins were seized by the FBI. Further backtracking of the 15 addresses which are believed by the FBI to belong to DPR are shown in Figure 5.

The remaining 4 addresses at the bottom of Figure 3 behave differently. From right to left are shown: two addresses which contributed 8,361 bitcoins which had been accepted on August 21, 2013 from one transaction of 1,010 bitcoins involving four medium sized amounts and two other transactions of 7,351 bitcoins involving 244 small amounts. Next to the left, there is one address with 2,000 bitcoins and another with 10,000, both originating in July, 2013.

Figures 3 and 5 summarize all the large-amount transactions which contributed bitcoins to accounts that the FBI believes were owned by DPR. We stopped the backtracking when the amounts became too small or when the number of involved addresses became too large. We traced 30 such origins: seven already appear in Figure 3: six on the right on top of the published address and one entering it from the left. The other 24 are shown in Figure 5. For instance, the nine transactions in the top-left took place already in 2012 and contributed 60,102 BTCs to a single address. Interestingly, four addresses had at some point

many more bitcoins than the number finally seized by the FBI. These addresses are marked by a brown cloud.

In Table 1 we summarize all the incoming transactions which seemingly belonged to DPR that our analysis discovered. We arranged them according to the month (left most column) they entered the accounts. For each month, from left to right, we describe the total number of received BTCs; the total number of transactions (how many transactions involving only small amounts and how many involving medium amounts); how many accounts participated in those transactions (small and medium amounts); how many BTCs were seized on 25/10/12 and finally how many BTCs were moved by DPR prior to his arrest. An interesting observation is that there is a huge variability in the amount he earned which we are aware of, which is inconsistent with the reasonable assumption that the total volume of business carried out on Silk Road was increasing at a roughly constant rate. In particular, the months of May, June and September 2013 are completely missing from this list. Assuming that DPR continued to receive at least some commissions from Silk Road during these months, it seems likely that he was simply using a different computer during these periods, which the FBI had not found or was unable to penetrate. In addition, it is evident that about a third of the bitcoins in these accounts, were moved out prior to his arrest. As it is believed that the Silk Road marketplace generated sales revenue of more than 9.5 million bitcoins with an average commission rate of 6.67%, we can conclude that he received about 633,000 BTCs in commissions. Consequently, the amounts seized by the FBI represent only about 22% of these commissions, while the amounts that we have identified, which are depicted in our figures, seem to represent about a third.

4 Is There a Close Connection Between Satoshi Nakamoto and DPR?

Further backtracking one particular transfer to the DPR-controlled address marked by the purple triangle on the top-right of Figure 5 reveals a very surprising connection involving considerable amounts of money between this account and an account which was created in the very early days of the Bitcoin scheme. It involves the recent transfer of 1,000 bitcoins, which was worth more than 60,000 dollars when it was made on march 20-th 2013, and close to a million dollars at today's exchange rate. Such a single large transfer does not represent the typical behaviour of a buyer who opens an account on Silk Road in order to purchase some narcotics (such buyers are expected to make an initial deposit of tens or hundreds of dollars, and to top the account off whenever they buy additional merchandise). It could represent either large scale activity on Silk Road, or some form of investment or partnership, but this is pure speculation.

The very early account we refer to was created on January 16-th 2009 (the leftmost account in Figure 6). This is just one week after block number 1 was mined on January 9-th 2009, after which regular mining operations commenced. It accumulated into it over 77,600 BTCs (mostly from mining operations) un-

til 19/5/2011. Its first transaction was the receipt of two amounts of 50 BTCs which were mined on 13/1/2009 and on 14/1/2009, just four and five days after block number 1 was mined. It has 25 incoming transactions which appear on block numbers smaller than 20,000, which mostly represent the consolidation of multiple awards of 50 bitcoins from mining operations. Collectively, these transactions contain about 715 awards which sum up to 35,775 bitcoins (representing about 46% of the entire sum). During June 2011 (4/6/2011-28/6/2011) almost all of these bitcoins were removed. In particular, 40,200 BTCs were moved to one account on June 14-th 2011 (the second leftmost). It is interesting to notice that the leftmost account continued to be actively managed, but its owner checked it only infrequently: On June 28-th 2011 its balance was reduced to 0.001 bitcoin and its owner noticed it and emptied the account on August 24-th 2011. For some reason (mistake? a tracking attempt?) the account received a tiny amount of 1 Satoshi (10^{-8} bitcoins) almost a year later on July 23-rd 2012. Its owner noticed this non-zero balance one year later, and emptied it once more on August 6-th 2013. On September 11-th 2013 he received another tiny transfer of 0.0000091, and on November 18-th 2013 yet another one of 0.00011. On November 20-th he sends the 0.0000091 but the 0.00011 is still there.

The Bitcoin community believes [9] that the vast majority of the early mining operations were carried out by Satoshi Nakamoto, and that during this early period he accumulated about one million bitcoins (which are currently worth close to a billion dollars) by mining most of the first 20,000 blocks. However, very little is known about his activities during this early period, since he rarely communicated with his colleagues via email, and all his communication stopped in 2010. Some web posts even speculated (without any proof whatsoever) that Satoshi Nakamoto died and took the secret keys needed to use his bitcoins to his grave.

The short path we found (which is depicted in Figure 6) suggests (but does not prove) the existence of a surprising link between the two mysterious figures of the Bitcoin community, Satoshi Nakamoto and DPR. It is reasonable to assume that all the accounts described along the top of Figure 6 belong to the same person, but to be on the safe side we refer to him as a “Founder” rather than as Satoshi Nakamoto. We are sure that analyzing this figure will start a very vigorous debate in the Bitcoin community.

Acknowledgments. This research was supported by a research grant provided by the Citi Foundation. We would like to thank Ronen Basri, Uriel Feige, Michal Irani, Robert Krauthgamer, Boaz Nadler, Moni Naor and David Peleg from the Computer Science and Applied Mathematics Department of the Weizmann Institute of Science for many interesting and informative discussions. We would also like to thank Aharon Friedman for his help in acquiring and processing the bitcoin data base. Finally, we would like to thank all the members of the Bitcoin community that we talked to, and especially Meni Rosenfeld.

References

1. The United States attorney's office: Manhattan U.S. Attorney Announces Seizure Of Additional \$28 Million Worth Of Bitcoins Belonging To Ross William Ulbricht, Alleged Owner And Operator Of Silk Road Website, 25 October 2013, <http://www.justice.gov/usao/nys/pressreleases/October13/SilkRoadSeizurePR.php>
2. Nakamoto, S.: Bitcoin: A Peer-to-Peer Electronic Cash System, 2008.
3. The blockexplorer: <http://blockexplorer.com/>
4. Ron D. and Shamir A.: Quantitative Analysis of the Full Bitcoin Transaction Graph. In Proceedings of the 17th International Conference on *Financial Cryptography and Data Security* in Okinawa, Japan, 2013. Springer-Verlag, A.-R. Sadeghi (Ed.): FC 2013, LNCS 7859, pp. 6-24, Berlin Heidelberg, 2013. <http://eprint.iacr.org/2012/584.pdf>
5. NPR Staff: Silk Road: Not Your Father's Amazon.com, 12 June 2011, <http://www.npr.org/2011/06/12/137138008/silk-road-not-your-fathers-amazon-com>
6. Greenberg A.: 'Silk Road 2.0' Launches, Promising A Resurrected Black Market For The Dark Web , Forbes, 6 November 2013, <http://www.forbes.com/sites/andygreenberg/2013/11/06/silk-road-2-0-launches-promising-a-resurrected-black-market-for-the-dark-web/>
7. Cox J.: GOOD NEWS, DRUG USERS - SILK ROAD IS BACK! , 6 November 2013, <http://www.vice.com/read/good-news-drug-users--silk-road-is-back>
8. Greenberg A.: FBI Says It's Seized \$28.5 Million In Bitcoins From Ross Ulbricht, Alleged Owner Of Silk Road, Forbes, 25 October 2013, <http://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/>
9. Lerner S. D.: The Well Deserved Fortune of Satoshi Nakamoto, Bitcoin creator, Visionary and Genius, Bitslog, 17 april 2013, <http://bitslog.wordpress.com/2013/04/17/the-well-deserved-fortune-of-satoshi-nakamoto/>