The electronic currencies networks: a pseudo-anonymous electronic currency system.

Abstract

Anonymity in the electronic currencies networks is a complicated issue. Usually users are identified by public-keys only. An attacker wishing to disclose anonymous will attempt to construct the one-to-many mapping between users and public-keys and associate information external to the system with the users. Electronic currencies networks tries to prevent this attack by storing the mapping of a user to his or her public-keys on that user's node only and by allowing each user to generate as many public-keys as required. One considers that the topological structure of the networks is derived from electronic currencies networks public transaction history. One shows that the two networks have a non-trivial topological structure, provide complementary views of the electronic currencies networks system and have implications for anonymity. One combines these structures with external information and techniques such as context discovery and own analysis to investigate an alleged theft of electronic currencies networks, which, at the time of the theft, had a market value of approximately half a million U.S. dollars.

Key words: network analysis, anonymity, electronic currencies.

Bitcoin is a peer-to-peer electronic currency system [1]. It relies on digital signatures to prove ownership and a public history of transactions to prevent double-spending. The history of transactions is shared using a peer-to-peer network and is agreed upon using a proof-of-work system [2]. The first Bitcoins were transacted in January 2009 and by June 2011 there were 6.5 million Bitcoins in circulation among an estimated 10,000 users [3]. In recent months, the currency has seen rapid growth in both media attention and market price relative to existing currencies. At the same time, lobby has raised concerns regarding the un-traceability of electronic currencies networks and their potential to harm society through tax evasion, money laundering and illegal transactions. The implications of the decentralized nature of electronic currencies networks for authorities' ability to regulate and monitor the owner of currency are as yet unclear. Many users adopt electronic currencies networks for political and philosophical reasons, as much as pragmatic ones. There is an understanding amongst electronic currencies networks more technical users that anonymity is not a prominent design goal of the system; however, opinions vary widely as to how anonymous the system is, in practice. A member of electronic currencies networks cannot be easily tracked back to you, and are a safer and faster alternative to other donation methods. development team is quoted as saying it would be unwise to attempt major illicit transactions with electronic currencies networks, given existing statistical analysis techniques deployed in the field by law enforcement; however, prior to this work, no analysis

of anonymity in electronic currencies networks was publicly available to substantiate or refute these claims. Furthermore, many other users of the system do not share this belief. An international organization for anonymous whistleblowers, recently advised its Twitter followers that it now accepts anonymous donations via electronic currencies networks and states that electronic currencies networks is a secure and anonymous digital currency electronic currencies networks cannot be easily tracked back to you, and are a safer and faster alternative to other donation methods. They proceed to describe a more secure method of donating electronic currencies networks that involves the generation of a one-time public-key but the implications for those who donate using the tweeted public-key are unclear. Is it possible to associate a donation with other electronic currencies networks transactions performed by the same user or perhaps identify them using external information? The extent to which this anonymity holds in the face of determined analysis remains to be tested. We consider some existing work relating to electronic currencies and anonymity. The economic aspects of the system, interesting in their own right, are beyond the scope of this work. An overview of the electronic currencies networks system is focused on three features that are particularly relevant to the analysis. Two network structures were constructed. Transaction network and user network are used the publicly available transaction history. The static and dynamic properties of these networks were studied for anonymity. Information external to the Bitcoin system was also combined with techniques such as flow and temporal analysis to illustrate how various types of information leakage can contribute to the de-anonymization of the system's users. The motivation for this analysis is not to de-anonymize individual users of the electronic currencies networks system. Rather, it is to demonstrate, using a passive analysis of a publicly available dataset, the inherent limits of anonymity when using electronic currencies networks. This will ensure that users do not have expectations that are not being fulfilled by the system. In security-related research, there is considerable tension over how best to disclose vulnerabilities [4]. Many researchers favor full disclosure where all information regarding the vulnerability is promptly released. This enables informed users to promptly take defensive measures. Other researchers favor limited disclosure; while this provides attackers with a window in which to exploit uninformed users, a mitigation strategy can be prepared and implemented before public announcement, thus limiting damage, e.g. through a software update. Our analysis illustrates some potential risks and pitfalls with regard to anonymity in the electronic currencies networks system. However, there is no central authority which can fundamentally change the system's behavior. Furthermore, it is not possible to mitigate analysis of the existing transaction history. There are also two noteworthy features of the dataset when compared with, say, contentious social network datasets, e.g. the Facebook profiles of students. Firstly, the delineation between what is considered public and private is clear: the entire history of electronic currencies networks transactions is publicly available. Secondly, the electronic currencies networks system does not have a usage policy. After joining electronic currencies networks peer-to-peer network, a client can freely request the entire history of electronic currencies networks

transactions; there is no crawling or scraping required. Thus, we believe the best strategy to minimize the threat to user anonymity is to be descriptive about the risks of the electronic currencies networks system. We do not identify individual users - apart from those in the case study- but we note that it is not difficult for other groups to replicate our work. Indeed, given the passive nature of the analysis, other parties may already be conducting similar analyses. The related work for this analysis can be categorized into two fields: electronic currencies and anonymity. Electronic currencies can be technically classified according to their mechanisms for establishing ownership, protecting against double-spending, ensuring anonymity and/or privacy, and generating and issuing new currency. Electronic currencies networks are particularly noteworthy for the last of these mechanisms. The proof-of-work system [5, 6] that establishes consensus regarding the history of transactions also doubles as a minting mechanism. The scheme was first outlined in the B-Money Proposal [7]. We briefly consider some alternative mechanisms. Ripple [8] is an electronic currency where every user can issue currency. However, the currency is only accepted by peers who trust the issuer. Transactions between arbitrary pairs of users require chains of trusted intermediaries between the users. Saito [9] formalized and implemented a similar system, i-WAT, in which the chain of intermediaries can be established without their immediate presence using digital signatures. KARMA [10] is an electronic currency where the central authority is distributed over a set of users that are involved in all transactions. PPay [11] is a micropayment scheme for peer-to-peer systems where the issuer of the currency is responsible for keeping track of it. However, both KARMA and PPay may incur a large overhead when the rate of transactions is high. A smart-card electronic currency preserves a central bank's role in the generation and issuance of electronic currency. A smart-card electronic currency was an electronic replacement for cash in the physical world whereas Bitcoin is an electronic analog of cash in the online world. The author is not aware of any studies of the network structure of electronic currencies. However, there are such studies of physical currencies. A community currency was introduced for a three-month period in a bid to revitalize local economy. The system involved gift-certificates that were re-usable and legally redeemable into the official currency. There was an entry space on the reverse of each certificate for recipients to record transaction dates, their names and addresses, and the purposes of use, up to a maximum of five recipients. Kichiji and Nishibe [12] used the collected certificates to derive a network structure that represented the flow of currency during the period. They showed that the cumulative degree distribution of the network obeyed a power-law distribution, the network had small-world properties (the average clustering coefficient was high whereas the average path length was low), the directionality and the value of transactions were significant features, and the double-triangle system [13] was effective. There also exist studies of the physical movement of currency [16] is a crowd-sourced method for tracking U.S. dollar bills where users record the serial numbers of bills in their possession, along with their current location. If a bill is recorded sufficiently often, its geographical movement can be tracked over time. This dataset was used as a proxy for studying multi-scale human mobility and as a

tool for computing geographic borders inherent to human mobility [17]. Greatest risk for electronic currencies networks developers, exchanges, wallet providers, mining pool operators and businesses is requiring certain kinds of financial businesses, even if they are located abroad, to register with a bureau of the United States Department of the Treasury known as the Financial Crimes Enforcement Network [24]. The question of legality of electronic currencies networks is outside the scope of this work but is interesting nonetheless. Previous work has shown the difficulty in maintaining anonymity in the context of networked data and online services which expose partial user information. The authors [13] consider privacy attacks which identify users using the structure of networks and show the difficulty in guaranteeing anonymity in the presence of network data. Crandall et al. [14] infer social ties between users where none are explicitly stated by looking at patterns of co-incidences or common off-network co-occurrences. Gross and Acquisiti [15] discuss privacy of early users in the Facebook social network, and how information from multiple sources could be combined to identify pseudonymous network users. Narayanan and Shmatikov [13] de-anonymized the Netix Prize dataset using information from IMDB3 which had similar user content, showing that statistical matching between different, but related datasets can be used to attack anonymity. Puzis et al. [18] simulated the monitoring of a communications network using strategically-located monitoring nodes and showed that, using real-world network topologies, a relatively small number of nodes can collaborate to pose a significant threat to anonymity. Korolova et al. [19] study strategies for efficiently compromising network nodes, to maximize link information observed. Altshuler et al. [21] discuss the increasing dangers of attacks targeting similar types of information, and provide measures of the difficulty of such attacks, on particular networks. All of this work points to the difficulty in maintaining anonymity where network data on user behaviour is available and illustrates how seemingly minor information leakages can be aggregated to pose significant risks. The security researcher Dan Kaminsky independently performed an investigation of some aspects of anonymity in the electronic currencies networks system, which he presented at a security conference [22] shortly after an initial draft of this work was made public. His work investigates the linking problem. In addition to the analysis we conducted, his work investigates the electronic currencies networks system from an angle we did not consider in our investigation - the TCP/IP operation of the underlying peer-to-peer network. Kaminsky's TCP/IP layer findings strengthen the core claims of this work that electronic currencies network does not anonymise user activity. Bitcoin is an electronic currency with no central authority or issuer. There is no central bank or fractional reserve system controlling the supply of electronic currencies networks. Instead, they are generated at a predictable rate such that the eventual total number will be 21 million. There is no requirement for a trusted third-party when making transactions. Suppose Alice wishes to send a number of Bitcoins to Bob. Alice uses a Bitcoin client to join the Bitcoin peer-to-peer network and makes a public transaction or declaration stating that one or more identities that she controls (which can be verified using public-key cryptography), and which previously had a

number of Bitcoins assigned to them, wish to re-assign those Bitcoins to one or more other identities, at least one of which is controlled by Bob. The participants of the peer-to-peer network form a collective consensus regarding the validity of this transaction by appending it to the public history of previously agreed-upon transactions (the block-chain). This process involves the repeated computation of a cryptographic hash function so that the digest of the transaction, along with other pending transactions, and an arbitrary nonce, has a specific form. This process is designed to require considerable computational effort, from which the security of the electronic currencies networks mechanism is derived. To encourage users to pay this computational cost, the process is incentivized using newly generated electronic currencies networks and/or transaction fees, and so this whole process is known as mining. There are three features of the electronic currencies networks system that are of particular interest. Firstly, the entire history of electronic currencies networks transactions is publicly available. This is necessary in order to validate transactions and prevent double-spending in the absence of a central authority. The only way to confirm the absence of a previous transaction is to be aware of all previous transactions. The second feature of interest is that a transaction can have multiple inputs and multiple outputs. An input to a transaction is either the output of a previous transaction or a sum of newly generated electronic currencies networks and transaction fees. A transaction frequently has either a single input from a previous larger transaction or multiple inputs from previous smaller transactions. Also, a transaction frequently has two outputs: one sending payment and one returning change. Thirdly, the payer and payee(s) of a transaction are identified through public-keys from public-private key-pairs. However, a user can have multiple public-keys. In fact, it is considered good practice for a payee to generate a new public-private key-pair for every transaction. Furthermore, a user can take the following steps to better protect their identity: they can avoid revealing any identifying information in connection with their public-keys; they can repeatedly send varying fractions of their Bitcoins to themselves using multiple (newly generated) public-keys; and/or they can use a trusted third-party mixer or laundry. However, these practices are not universally applied. The three features above, namely the public availability of Bitcoin transactions, the input-output relationship between transactions and the reuse and co-use of public-keys, provide a basis for two distinct network structures: the transaction network and the user network. The transaction network represents the flow of Bitcoins between transactions over time. The transaction network T represents the flow of Bitcoins between transactions over time. It is a straight-forward task to construct T from a dataset. The user network U represents the flow of Bitcoins between users over time. You need to perform a preprocessing step before you can construct U from a dataset. The difficulty is that public-keys are Bitcoin's mechanism for ensuring anonymity. The public can see that someone identified by a public-key is sending an amount to someone else identified by another public-key, but without information linking the transaction to anyone [20]. In fact, it is considered good practice for a payee to generate a new public - private key-pair for every transaction to keep transactions from being linked to a common owner. Therefore,

it is impossible to completely perfect the network using our dataset alone. However, some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner [20]. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner. The network's growth and sparsification are evident. One note that even though dynamic analysis of the user network is on a monthly basis, the preprocessing step is performed using the ancillary network of the entire incomplete network. This enables us to resolve public-keys to a single user irrespective of the month in which the linking transactions occur. The contraction of public-keys into users, while incomplete, generates a network that is in many ways a proxy for the social network of Bitcoin users. The edges represent financial transactions between pairs of users. It may be possible to identify, for example, communities, central users and hoarders within this social network. Prior to performing the analyses above, one expected the user network to be largely composed of trees representing Bitcoin flows between one-time public-keys that were not linked with other public-keys. However, our analyses reveal that the user network has considerable cyclic structure. One now consider the implications of this structure, coupled with other aspects of the Bitcoin system, for anonymity. There are several ways in which the user network can be used to deduce information about Bitcoin users. One can use global network properties, such as degree distribution, to identify outliers. One can use local network properties to examine the context in which a user operates by observing the users with which he or she interacts with either directly or indirectly. The dynamic nature of the user network also enables us to perform flow and temporal analyses. One can examine the significant Bitcoin flows between groups of users over time. One will now discuss each of these possibilities in more detail and provide a case study to demonstrate their use in practice. There is no user directory for the Bitcoin system. However, one can attempt to build a partial user directory associating Bitcoin users (and their known public-keys) with off-network information. If we can make sufficient associations and combine them with the network structures above, a potentially serious threat to anonymity emerges. Many organizations and services such as on-line stores that accept Bitcoins, exchanges, laundry services and mixers have access to identifying information regarding their users, e.g. e-mail addresses, shipping addresses, credit card and bank account details, IP addresses, etc. If any of this information is publicly available, or accessible by, say, law enforcement agencies, then the identities of users involved in related transactions may also be at risk. To illustrate this point, we consider a number of publicly available data sources and integrate their information with the user network. The Bitcoin Faucet [23] is a website where users can donate Bitcoins to be redistributed in small amounts to other users. In order to prevent abuse of this service, a history of recent giveaways is published along with the IP addresses of the recipients. When the Bitcoin Faucet does not batch the redistribution, it is possible to associate the IP addresses with the recipient's public-keys. This page can be scraped over time to produce a time-stamped mapping of IP addresses to users. The public-keys associated with many of the IP addresses that received Bitcoins were contracted

with other public-keys in the ancillary network, thus revealing IP addresses that are somehow related to previous transactions. There is a map of geo located IP addresses belonging to users who received Bitcoins over a period of one week. The corresponding users are linked by an undirected path of length at most three in the user network. Large centralized Bitcoin service providers are capable of producing much more detailed maps. Map of geo located IP addresses associated with users receiving Bitcoins from the Bitcoin Faucet during a one week period. A map of a sample of the geo located IP addresses in connected by edges, where the corresponding users are connected by a path of length at most three in the user network, that does not include the vertex representing the Bitcoin Faucet. Another source of identifying information is the voluntary disclosure of public-keys by users, for example, when posting to the Bitcoin forums. Bitcoin public-keys are typically represented as strings approximately thirty-three characters in length and starting with the digit one. They are indexed very well by popular search engines. One identified many high-degree vertices with external information using a search engine alone. We scraped the Bit- coin Forums where users frequently attach a public-key to their signatures. One also gathered public-keys from Twitter streams and user-generated public directories. It is important to note that in many cases you are able to resolve the `public' public-keys with other public-keys belonging to the same user using the ancillary network. We also note that large centralized Bitcoin service providers can do the same with their user information. Security researcher Dan Kaminsky has performed an analysis of the Bitcoin system, investigating identity leakage at the TCP/IP layer. He found that by opening a connection to all public peers in the network at once, he could map IP addresses to Bitcoin public-keys, working from the assumption that, the first node to inform you of a transaction is the source of it. This is more or less true, and absolutely over time [22]. Using this approach it is possible to map public-keys to IP addresses unless users are using an anonymising proxy technology such as TOR. There are several pieces of information we can directly derive from the user network regarding a particular user. One can compute the balance held by a single public-key. One can also aggregate the balances belonging to public-keys that are controlled by a particular user. The donations are relatively small and are forwarded to other public-keys periodically. There was also a noticeable spike in donations when the facility was first announced. An important advantage of deriving network structures from the Bitcoin transaction history is our ability to use network visualization and analysis tools to investigate the flow of Bitcoins. The network structure surrounds the WikiLeaks' public-key in the incomplete user network. At the time of theft, the stolen Bitcoins had a market value of approximately half a million U.S. dollars. One chose this case study to illustrate the potential risks to the anonymity of a user (the thief) who has good reason to remain anonymous. One considers the incomplete user network before any contractions. One restricts ourselves to the egocentric network surrounding the thief: we include every vertex that is reachable by a path of length at most two ignoring directionality and all edges induced by these vertices. One also removes all loops, multiple edges and edges that are not contained in some bi-connected component to avoid clutter. An

interesting sub-network induced by the thief, the victim. Interestingly, the victim and the thief are joined by paths. Sub-network is a cycle. This allows us to attach values in Bitcoins and timestamps to the directed edges. One can make a number of observations. The theft of 25 000BTC was preceded by a smaller theft of 1 BTC. This was later reported by the victim in the Bitcoin forums. There has been at least one attempt to associate the thief with LulzSec [13]. This was a fake; it was created after the theft. The victim, he is a member of the Slush pool, and like the thief, he is a one-time donator to LulzSec. This donation, the day before the theft, is his last known activity using these public-keys. One can follow significant flows of value through the network over time. If a vertex representing a user receives a large volume of Bitcoins relative to their estimated balance, and, shortly after, transfers a significant proportion of those Bitcoins to another user, we deem this interesting. Special purpose tool starting with a chosen vertex or set of vertices traces significant flows of Bitcoins over time. In practice we have found this tool to be quite revealing when analyzing the user network. The victim has developed their own tool to generate an exhaustive list of public-keys that have received some portion of the stolen Bitcoins since the theft. However, this list grows very quickly and, at the time of writing, contained more than 34 100 public-keys. The initial theft of a small volume of 1 BTC is immediately followed by the theft of 25000 BTC. The flows split and later merge, validating that the flows found by the tool are probably still controlled by a single user. There are several other examples of interesting flow. The Bitcoins are transferred between public-keys along the paths very quickly. Much of this analysis is circumstantial. One cannot say for certain whether or not these flows imply a shared agency in both incidents. However, it does illustrate the power of our tool when tracing the flow of Bitcoins and generating hypotheses. It also suggests that a centralized service may have further details on the user(s) in control of the implicated public-keys. There are many other forms of analysis that can be applied in order to disclose the anonymous workings of the Bitcoin system. Many transactions have two outputs: one is the payment from a payer to a payee and the other is the return of change to the payer. If we assume that a transaction was created using a particular client implementation and we have access to the client's source code, then we may be able to deduce, in some cases, which was the output and which was the change. One can then map the public-key that the change was assigned to back to the user who created the transaction. Order books for Bitcoin exchanges are typically available to support trading tools. As orders are often placed in Bitcoin values converted from other currencies, they have a precise decimal value with eight significant digits. It may be possible to find transactions with corresponding amounts and thus map public-keys and transactions to the exchanges. Over an extended time period, several public-keys, if used at similar times, may belong to the same user. It may be possible to construct and cluster a co-occurrence network to help deduce mappings between public-keys and users. Finally, there are far more sophisticated forms of attack where the attacker actively participates in the network, for example, using marked Bitcoins or by operating a laundry service. In addition to educating users about the limits of anonymity in the Bitcoin system,

some risks to privacy could potentially be mitigated by making changes to the system. A patch to the official Bitcoin client has been developed, which allows users to prevent the linking of public-keys by making the user aware of potential links within the Bitcoin client user-interface. It is also possible for the client to automatically proxy Bitcoins through dummy public-keys. This would come at the cost of increased transaction fees but would increase deniability and obfuscate the chain of transaction histories. Finally, if a future version of the protocol supported protocol-level mixing of Bitcoins, this would increase the difficulty for a passive third-party to track individual user histories. For the past half-century futurists have heralded the advent of a cashless society. Many of their predictions have been realized, e.g. on-line real-time payment system and bank-maintained central information files. However, cash is still a competitive and relatively anonymous means of payment. Bitcoin is an electronic analog of cash in the online world. It is decentralized: there is no central authority responsible for the issuance of Bitcoins and there is no need to involve a trusted third-party when making online transfers. However, this flexibility comes at a price: the entire history of Bitcoin transactions is publicly available. In this chapter we investigated the structure of two networks derived from this dataset and their implications for user anonymity. Using an appropriate network representation, it is possible to associate many public-keys with each other, and with external identifying information. With appropriate tools, the activity of known users can be observed in detail. This can be performed using a passive analysis only. Active analyses, where an interested party can potentially deploy marked Bitcoins and collaborate with other users can discover even more information [25]. Large centralized services such as the exchanges and wallet services are capable of identifying and tracking considerable portions of user activity. Technical members of the electronic currency network community have cautioned that strong anonymity is not a prominent design goal of the electronic currency network system. However, casual users need to be aware of this, especially when sending electronic currency to users and organizations they would prefer not to be publicly associated with [26]. NetCash is the USC Anonymous network payment research prototype. The NetCash research prototype is a framework for electronic currency developed by Clifford Neuman and Ari Medvinsky at the Information Sciences Institute of the University of Southern California. NetCash will enable new types of services on the Internet by providing a real-time electronic payment system that satisfies the diverse requirements of service providers and their users. Among the properties of the NetCash framework are security, anonymity, scalability, acceptability, and interoperability. NetCash was designed to facilitate anonymous electronic payments over an unsecure network without requiring the use of tamper-proof hardware. NetCash provides secure transactions in an environment where attempts at illegal creation, copying, and reuse of electronic currency are likely. In order to protect the privacy of parties to a transaction, NetCash implements financial instruments that prevent traceability and preserve the anonymity of users. NetCash and NetCheque is a great combination. When used in combination with NetCheque, service providers and their users are able to select payment mechanisms based on the level of anonymity

desired, ranging from non-anonymous and weakly anonymous instruments that are scalable, to unconditionally anonymous instruments that require more resources of the currency server. NetCash provides scalable electronic currency that is accepted across multiple administrative domains. Currency issued by a currency server is backed by account balances registered with NetCheque to the currency server itself. NetCash currency servers also use the NetCheque system to clear payments across servers, and to convert electronic currency into debits and credits against customer and merchant accounts. Though payments using NetCheque originate from named accounts, with NetCash the account balances are registered in the name of the currency server, and not the end user. Since the introduction of the NetCash research prototype, there have been several other payment systems that have used the NetCash name. Over time, samples of these systems have operated at netcash.com. None of these other systems are affiliated with the NetCash research prototype [27].

References

1. http://bitcoin.org/ (дата обращения: 04.08.12).
2. http://ru.wikipedia.org/wiki/Bitcoin#cite_note-whitepaper-1 (дата обращения: 07.08.12).
3. http://arxiv.org/pdf/1107.4524.pdf (дата обращения: 07.08.12).
4. Cavusoglu, H., Cavusoglu, H., Raghunathan, S. (2005). Emerging Issues in Responsible Vulnerability Disclosure. Proceedings of the 4th Workshop on the Economics of Information Security, Boston, MA, 2005.
5. http://www.hashcash.org/papers/hashcash.pdf
6. http://e-archivo.uc3m.es/bitstream/10016/5057/1/EPALOMAR_THESIS.pdf
7. http://www.weidai.com/bmoney.txt
8. http://ripple-project.org/
9. K. Saito. i-WAT: The Internet WAT System { An Architecture for Maintaining Trust and Facilitating Peer-to-Peer Barter Relationships. PhD thesis, Keio University, 2006.
10. Karma: A secure economic framework for p2p resource sharing V Vishnumurthy, S Chandrakumar, EG Sirer Workshop on Economics of Peer-to-Peer Systems
11. http://ilpubs.stanford.edu:8090/757 (дата обращения: 05.08.12).
12. http://cc.econ.hokudai.ac.jp/en/system/files/nacfcc.pdf
13. http://www.informatik.uni-trier.de/~ley/db/indices/a-tree/s/Shmatikov:Vitaly.html
14. http://www.pnas.org/content/107/52/22436.figures-only

15. Gross R., Acquisti A. Information Revelation and Privacy in Online Social Networks. //In Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society, pages 71-80. ACM, 2005.
16. http://www.wheresgeorge.com/
17. D. Brockmann, L. Hufnagel, and T. Geisel. The Scaling Laws of Human Travel. Nature, 439(26):462-465, 2006.
18. R. Puzis, D. Yagil, Y. Elovici, and D. Braha. Collaborative Attack on Internet Users' Anonymity. Internet Research, 19(1):60-77, 2009.
19. A. Korolova, R. Motwani, S. Nabar, and Y. Xu. Link Privacy in Social Networks. In Proceedings of the 17th ACM Conference on Information and Knowledge Management, pages 289-298. ACM, 2008.
20. http://bitcoin.org/bitcoin.pdf (дата обращения: 08.08.12).
21. Y. Altshuler, N. Aharony, Y. Elovici, A. Pentland, and M. Cebrian. Stealing Reality: When Criminals Become Data Scientists (or Vice Versa). Intelligent Systems, 26(6):22-30, 2011.
22. D. Kaminsky. Black Ops of TCP/IP Presentation. Black Hat, Chaos Communication Camp, 2011.
23. https://freebitcoins.appspot.com/
24. http://www.fincen.gov/
25. http://osaka.law.miami.edu/~froomkin/articles/tcmay.htm
26. http://www.cfp.org/2012/wiki/index.php/CFP_Mini-Conferences
27. http://www.bcneuman.com/ecommerce/