GdPO Global Drug Policy Observatory
reporting monitoring analysis

LRC Language Research Centre
CYI Canolfan Ymchwil Iaith

ISSN 2054-1910

Swansea University
Prifysgol Abertawe

Hard Interventions and Innovation in Crypto-Drug Markets: The escrow example

Martin Horton-Eddison[1*] & Matteo Di Cristofaro[2¥]

Policy Brief 11 | August 2017

KEY POINTS

- Comparative analysis of mass data crawled from Silk Road and Silk Road 2.0 reveals that there is some evidence to corroborate assertions that ‘hard’ law enforcement practices may contribute to the adoption of specific technological innovations in crypto-drug markets

- Specifically, the study applied a corpus linguistics assisted discourse analysis methodology to crypto-drug market community attitudes toward *escrow* technologies. Although a subsequent theft of Bitcoin held in Silk Road 2.0’s escrow accelerated community determination to adopt innovated escrow solutions, initial concerns about the viability of this crucial trust technology were found to have their genesis in the period following law enforcement’s closure of the original Silk Road

- The analysis suggests that the FBI’s seizure of the original Silk Road may have fired the starting gun in the race to adopt decentralised escrow in crypto-drug markets. More broadly, ‘hard’ law enforcement strategies designed to support prohibition-orientated polices online may therefore be counter-productive to some degree

- When generalised, this specific example of a resultant breakdown in trust in traditional centralised escrow - and subsequent drive to adopt technological innovation - may also be true of other advances in crypto-drug markets technologies

[1] * PhD Researcher, Global Drug Policy Observatory
[2] ¥ Independent Post-doctoral Researcher

INTRODUCTION

Recent literature has produced a discourse of growing orthodoxy that short-term 'hard' law enforcement operations aimed at closing or seizing Crypto-Drug Markets (CDMs) serve only to drive medium to long-term CDM technological innovations in response. For instance, Mountenay, Griffiths, and Vandam suggest that 'police takedowns act as a catalyst for new security developments.'[1] Buxton and Bingham state that 'the effect of enforcement activities on the Dark Net has been to fragment and diversify drug markets, while catalysing innovation in security.'[2] *Prima face*, the orthodox view makes common sense, but it does not account for the effects of other events, such as scam events. If the emerging orthodoxy is to be held as fact, it must be investigated empirically.

This policy brief is intended to test the core hypothesis that so-called 'hard' law enforcement operations (i.e. site take-downs) are a significant cause for innovation of CDM technologies. Because the recent shift away from centralised escrow - toward decentralised escrow – represents a key CDM technological innovation direction,[3] CDM community attitudes to escrow innovation provide the study's dependent variable. Accordingly, the two independent variables are (i) the FBI's take-down of Silk Road 1.0, and (ii) the later Silk Road 2.0 transaction malleability scam. This brief therefore presents an analysis of user attitudes to escrow systems in a pair of given CDMs in the periods before, and after, the FBI's closure of Silk Road, and also accounts for the effects of the scam event. Escrow was chosen because, as a principal CDM trust technology, it is central to all market transactions, has evolved significantly since Silk Road, and at the time of writing, four of the five most popular CDMs now accommodate decentralised escrow.[4]

In order to provide the data required to measure the effect of the independent variables on the dependent, a Corpus Linguistics Assisted Discourse Analysis (CLADA) methodology was designed and operationalised. This facilitated a systematic comparative analysis of vast data sets from two key historic markets large data snapshots from the original Silk Road (SR1), and Silk Road 2.0 (SR2). The methodology is discussed in detail in the accompanying Situation Analysis.[5] To summarise the approach; changes in attitude to escrow were measured by contextual analysis of all instances of the term *escrow* in chat fora on both sites, yielding a data bank in excess of 70,000 escrow-related results, discussed in more detail in the results section.

Summarily, the study found that in the case of CDM escrow innovation, hard law enforcement operations contributed to the *initiation* of community discussions in favour of incorporating external escrow innovations in future CDMs. However, it should be noted that although the FBI's seizure of the original Silk Road may have fired the starting gun in the race towards adoption of decentralised escrow, innovation attitudes were further embedded and sustained in response to the second independent variable, that of Silk Road 2.0 exit scam. The study acknowledges that generalizability is limited by the analysis of just two case studies, and indeed one specific technology. Caveats notwithstanding, analysis of the data largely supports the law enforcement –innovation-catalyst thesis. The evidence suggests that hard law enforcement interventions *can* inaugurate innovation attitude shifts in CDM communities. But, they are not *entirely* responsible: market forces, most notably scams which result in the loss of crypto-currency, can also contribute to nurturing a sustained shift toward innovation adoption.

BACKGROUND TO TRUST IN CDMS

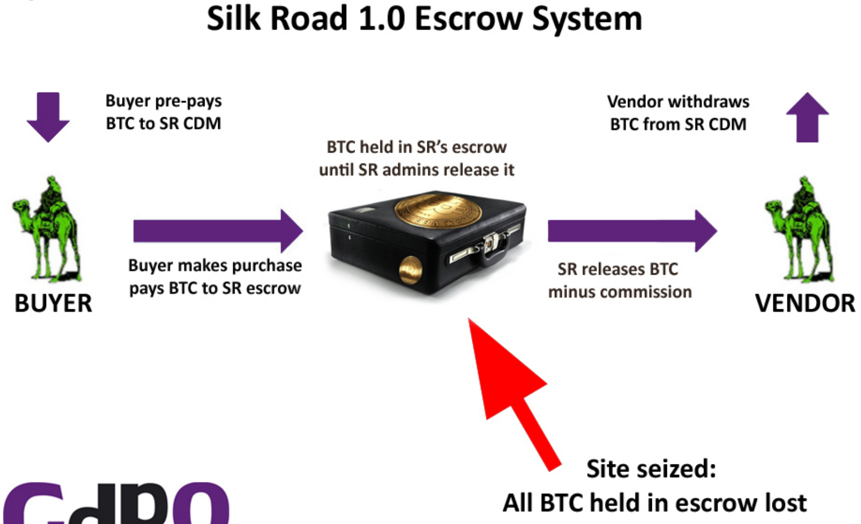
The prohibition dominated approach to non-medical and non-scientific use of certain psychoactive substances is a long-standing feature of international drug policy, but the trade in drugs online is a relatively new feature. Historic interventions by state and international law enforcement agencies against online drug transactions on the clearnet, combined with the increasingly de-anonymised nature of the internet in general, have driven the online drug trade underground, into cryptographically obscured spaces on the darknet. The oft-cited case of one such marketplace, the Silk Road website, and its subsequent closure has attracted the attention of law enforcement communities around the world; CDMs are now a limited but growing feature of drug policy literature and law enforcement considerations.

Engaging in the purchase or sale of goods in any online environment involves a significant element of trust because parties likely do not know, or ever meet, each other in the real world. This situation is further complicated in CDMs which depend on anonymising technologies, and which operate extra-judicially, often dealing in illegal or illicit goods. Compared with legitimate online commerce, illegality therefore increases the potential for intervention by law enforcement, with significant risk to both parties eroding the trust in the transaction process itself. Finally, all parties must trust that the CDM is capable of mediating the transaction in an environment secured against law enforcement activities, and that will not intentionally involve itself in defrauding either party – known as an 'exit scam.' CDM transactions therefore require three key areas of trust: trust between buyer and seller, trust that law enforcement can be evaded, and trust in the website to host the transaction honestly. This paper's analysis of the data shows that until its closure in October 2013, SR1 appeared to have the trust of its community. A combination of anonymising browser technologies (TOR), the use of the semi-obscured crypto-currency (Bitcoin), and transactional trust technologies (escrow) led to a widely-held belief that the site was largely impenetrable to law enforcement (LE), and that the site's intentions toward both buyers and vendors were honest. The website was therefore trusted to provide an escrow service – to act as an arbiter – and the escrow system was trusted in turn to adequately mitigate risk between buyer and vendor.

ESCROW

In its purest form, escrow simply means a deed held in trust by a third party until a further condition is satisfied. In CDM transactions, the further conditions are ordinarily limited to the delivery of the drugs from the vendor to the buyer. The SR1 escrow system is illustrated in Figure 1.0:

Figure 1.0


Silk Road 1.0 Escrow System
Buyer pre-pays BTC to SR CDM
BTC held in SR's escrow until SR admins release it
Vendor withdraws BTC from SR CDM
BUYER
Buyer makes purchase pays BTC to SR escrow
SR releases BTC minus commission
VENDOR
Site seized: All BTC held in escrow lost

GdPO Global Drug Policy Observatory
reportingmonitoringanalysis

Since their inception, the most popular payment currency used on CDMs has been Bitcoin (BTC), one of a host of crypto-currencies. BTC operates on the general bitcoin protocol. Payment using BTC is ordinarily managed through an escrow system which provides buyers and vendors with security and confidence[6] in the validity of transactions. In the case of SR1, escrow operations were *centralized*, i.e. monies were held by Silk Road itself until both parties (vendor and buyer) had agreed that all conditions of the transaction had be met to the satisfaction of both the vendor and the buyer (see figure 1.0). On SR1 and (eventually) SR2, the escrow process operated as such: the purchaser clicked to buy an item/s, BTCs were transferred from purchaser's Bitcoin 'wallet' and into trust (the website's wallet), the vendor then dispatched the product, upon receipt of the goods the purchaser then informed the site, and funds were transferred from the CDM wallet to the vendor, minus the CDM's commission. In this way, centralised escrow was employed to mitigate counterparty risk[7] by ensuring that transactions were fully completed to all parties' satisfaction.[8] Throughout the transaction process, the risk of buying and selling anonymously was mitigated by trust in the systemic processes, and in the administrators of the CDM. Indeed, as one user in the data suggested '…the beauty of escrow is that you don't have to trust them [vendors] I often try out new vendors, they are usually eager to impress you with their wares and service.' (For a selection of other quotes on usage of escrow see Appendix 2).

However, the seizure - and subsequent closure - of SR1 by the FBI in October 2013 resulted in the loss of $3.6million of site users' BTC pending sign-off in escrow. The centralised nature of the SR1 escrow process had therefore resulted in the loss of users' money in this instance; the very thing that it was designed to prevent in normal operations. As such, we can perceive of centralised escrow as a technical vulnerability, a point of failure in the traditional CDM model. By contrast, today's CDMs are moving rapidly toward total decentralisation; and this includes moves toward multisig escrow. For a detailed explanation of decentralised multisig escrow, see Horton-Eddison *Updating Escrow: Demystifying the CDM multisig process*.[9] The subsequent move toward adoption of these innovations by CDM communities correlates with the identified attitudinal shift toward decentralised escrow following the events described in this paper. As such, to identify the genesis of decentralised escrow adoption attitudes on CDMs specifically, provides some utility to those who wish to identify the origins of CDMs' adoption of other technological innovation more broadly.

METHODOLOGY

The analysis evidences large-scale communicative and social profiling of transactional behaviour in crypto-drug markets. The study utilised publically available data previously crawled from the original Silk Road, (SR1) and the subsequently launched Silk Road 2.0 market (SR2).[10] A bespoke Corpus Linguistics Assisted Discourse Analysis (CLADA) methodology was employed to analyse the data. This enabled the location of user perceptions of escrow on both sites (SR1 & SR2). This policy brief is associated with an accompanying GDPO *Situation Analysis*[11] which describes the methodology in greater detail. The methodology paper is available here. Briefly, the analysis integrated data-centred quantitative methods from Corpus Linguistics, and interpretative qualitative methods from Public Policy. The data was narrowed by application of the search term *escrow* to forum chat data on SR1 and SR2. This generated lists of the fora's most frequently co-occurring terms (collocates[12]). Secondary analysis located these terms in conversations (occurrences[13]). In total, the SR1 data snapshot provided 37,492 mentions of escrow. The SR2 data provided 34,293 total mentions of the escrow.

Of these, there were 3,493 statistically significant individual collocates of escrow in SR1, and 3,911 in the SR2 data. These were then further sorted into *(de)centralized* and *multi-signature* variants. Contextually, collocates were interpreted according to the chronology of historical events, such as the seizure of SR1, the opening of SR2, and the subsequent SR2 scam, described later. *Occurrence* data was used to provide wider context to the collocate data. Using embedded metadata, SR2 data was then further segmented into two tranches; before the major theft of Bitcoin from the site's escrow system (**SR2a**) on 13th February, 2014, and after that event (**SR2b**).[14] These separations were designed to permit independent assessment of (both vendors' and purchasers') reactions to each event in turn; thereby creating independent variables of the FBI seizure, and the later scam. Any detected shift in the escrow discourse could then be correctly attributed to the distinct events which defined each independent variable. Accordingly, the dependent variable – attitudes to escrow innovation – could be measured with greater accuracy. Finally, general SR1 data was used as a benchmark for normalised community attitudes to escrow before the seizure. Subsequent SR2**a** data provided a body of direct and related reactions to law enforcement's seizure of Silk Road. This SR2a data was drawn from the first months of SR2 operations – immediately after the FBI event, but before the scam event. SR2**b** data provided mixed reactions, which included responses to the closure of SR1, and the SR2 scam. SR2b data was drawn from the period after the scam, and includes the full period to the last day of SR2 operations. Summarily, changing attitudes toward escrow that occur between SR1 and SR2a can therefore be linked to the closure of SR1, and any SR2b shift might be linked to either the scam, the FBI event, or both.

RESULTS IN DETAIL

Generally speaking, the study found that in the broad SR1 data, the words most often collocated with escrow were positive terms associated with encouraging escrow usage; for example, the two most common were *in* and *stay*. More broadly, of the top one hundred collocates on SR1, there are few instances of words used in negative discourses referring to escrow, with the overwhelming majority positively encouraging its use. General trust in escrow throughout the lifespan of SR1 might therefore be considered high. By contrast, the general SR2 data evidences significant new collocates in the top 100 most often related to escrow. For example, the idea of finalising early (FE), that is, to work outside of escrow and to authorise release of payment from the purchaser to the vendor before the goods are received, climbed from 95th on SR1 to 52nd on SR2. This process was almost universally guarded against in the SR1 data. Similarly, *without*, (to engage in transactions without escrow) climbed to 13th on SR2, compared with 112th on SR1. The concept of *opt-out(to opt-out of escrow)* appeared at 64th on SR2 as an entirely new entry, having never appeared in the top one thousand on SR1. More specifically, in the period after the SR2 scam, the SR2b data evidenced a complete breakdown of trust in escrow; the idea of buyer/seller *disputes* appeared *at 82nd* in SR2, also never having appeared in the top one thousand on SR1. The idea to *remove* (escrow from the site) appeared at 95th on SR2, up from 515th on SR1. This evidenced increased community discussion about the perceived weakness of escrow in SR2, with concern over its continued viability after the events of SR1 and SR2a. Perhaps most tellingly, *centralized* appeared at 12th in SR2, and *decentralized* at 41st. When combined, (de)centralisation represented the most discussed forum topic on SR2. By contrast, neither word appeared in the top one thousand collocates of escrow on SR1 at all. SR2 data therefore evidenced a growing consensus toward moving away from centralised site-based escrow to decentralised escrow for future iterations of CDMs. However, these general trends included combined attitudinal shift in response to two key events – the FBI seizure and the BTC scam. To be meaningful for the original question – that of the effect on innovation of site-seizure by law enforcement - the SR2a data was isolated from SR2b data.

As mentioned, the terms *centralized*, *(de) centralized, multi-sig,* multisig, *multi-signature, or multisignature* did not collocate with escrow on SR1: there was therefore no significant link with *escrow* and any *(de)* centralization discussions (i.e. did not appear in the top one thousand collocates) before the FBI event. This is despite multisig being in development since February 2012, and practical iterations of the technology being publically available for use since August 2013,[15] at least two months before the seizure of the SR1 site. Notably, when the SR2a data was isolated from the SR2b data, it was revealed that combined *decentralisation* and *multisig* collocate data appeared among the top five collocates in the period after SR1 was seized. To a certain extent, this may be due to a more general emerging awareness of the new technology over the period. However, the timing of the upswing bears strong correlation to the independent variable chronology. The situation is further clarified when *occurrence* data is included to provide context. To provide just one example, there were 75 unique occurrences of *(de)centralization* of escrow in the SR2a data (after FBI seizure of SR1). This compares with 206 occurrences in the SR2b data (after the scam). It should be noted that SR2a data only occurs over a four month period, and SR2b data occurrences cover the later eight month period. When the SR2a occurrences and the SR2b occurrences are weighted to simulate an equalised time period, the SR2a data accounts for 42%, and the SR2b 58% of the decentralisation mentions proportionally. This study acknowledges that in general, discussion about new technologies naturally increases as awareness of that technology grows over time, and that this may account for the 16% swing toward decentralization in attitudes in the SR2b data. However, even with these factors considered, the effect of the FBI event appeared to be only slightly smaller than the effect of the subsequent scam event. Acknowledging that the FBI event occurred first, i.e. failure of escrow was novel at that stage, this seems to support to the catalysis thesis. Indeed, although lower in frequency, the SR2a instances may indicate that the FBI's closure of SR1 *instigated* discussions of escrow innovation, even if it appears that it was the scam that *progressed* the normalisation of a decentralisation innovation discourse. (See Appendix 1 for timelines and Appendix 3 for collocate and occurrence examples.)

SUMMARY

This study shows that instances of trust in centralised escrow were very high in SR1, with very limited criticism of the process, or of the CDM's technology, and with high levels of recommendation and adherence. In SR1, escrow's collocates were found to be generally used in - or linked to - positive discourses/attitudes, and did not include discussion of (de)centralisation or multisig innovation in any significant way. By contrast, general user attitudes to 'traditional' escrow on the SR2 site revealed a significantly less positive discourse. Indeed, when interrogated alongside the occurrence data, the SR2 data demonstrated the emergence of significant doubts in the security of centralised escrow systems in general, and an emerging consensus away from centralised escrow and toward decentralised escrow, and multi-signature systems specifically. Specific contextual analysis of elements of the SR2a occurrence data made notable mention of the FBI, seizure of servers, of servers being compromised, of shut down, of demise, and of the subsequent requirement for evolution of escrow. Some users even explicitly *hailed* the closure of SR1 because it precipitated innovation of technologies including escrow. Despite a level of escrow technological development occurring outside of the CDM sphere *before* the events measured in this paper, the near-total absence of discussion of these wider developments in the SR1 data is difficult to ignore. It suggests a lack of desire for innovation before the FBI event on SR1. Indeed, that such discussions occurred almost immediately in the SR2a data seems unlikely to be entirely coincidental. Accordingly, the closure of the original Silk Road website in October 2013 can be considered to have fired the starting gun on a technological game of cat and mouse in the CDM sphere - between those who are tasked with enforcing prohibition-orientated drug laws - and CDM users who desire to circumvent them. That said, it is acknowledged that this is just one example drown from time-specific data from just two CDMs. Whilst not definitive, the deteriorating attitudes to centralised escrow on SR2 compared with SR1 provide a salient case study for the effects of 'hard' law enforcement on the dark net. And, when generalized, may evidence a broader comprehensive relationship between hard enforcement strategies and CDM community attitudes to technological innovation in the round.

Summarily, law enforcement takedowns clearly play a catalytic role in innovation, but it is acknowledged that this may not necessarily be the only one. Nevertheless, this study raises questions over the long-term efficacy of 'hard' law enforcement strategies on the dark net, if those actions are intended to curb usage of CDM for drug transactions. The research highlights the potentially counter-productive nature of takedowns in particular. Policy practitioners may therefore ask a recurring question; just as in traditional drug markets, do short-term results, necessarily mean long term successes?

ACKNOWLEDGEMENTS

The authors would like to thank Professor Dave Bewley-Taylor, Director of the Global Drug Policy Observatory, Research Institute of Arts and Humanities, Swansea University, and Professor Nuria Lorenzo-Dus, English Language and Applied Linguistics, Swansea University for comments on earlier drafts of this policy brief. Thanks also for insightful feedback and comments received from the participants of the roundtable on 'Cyber-Trust in Crypto-Drug Markets: Implications for Policy and Policing' held at the International Institute for Strategic Studies, 4th April, 2017.^ The authors would also like to thank the CHERISH-DE initiative for supporting this research. Any errors of fact or interpretation remain with the authors.

^ For an account of the event, see Juan Fernandez Ochoa 'Trust in the Crypto-Drug Markets' http://gdpo.swan.ac.uk/?p=466

ENDNOTES

1 Mounteney, J., Griffiths, P. & Vandam, L., *What is the Future of Internet Drug Markets?* in EMCDDA. (eds.) *The Internet and Drug Markets*. Luxembourg: Publications Office of the European Union, 2016. P. 130

2 Buxton, J. & Bingham, T., *The Rise and Challenge of Dark Net Markets*, Policy Brief No.7, Global Drug Policy Observatory, January, 2015. P.12

3 Greenberg, A., *The Silk Road's Dark Web Dream is Dead*, Security, Wired.com, 14th January, 2016

4 Horton-Eddison, M., *Updating Escrow: demystifying the CDM multisig process*, GDPO Situation Analysis, GDPO, Swansea, July, 2017. P.1 Available: http://www.swansea.ac.uk/media/HortonEddisonGDPOMultiSigEscrowSA.pdf

5 Di Cristofaro, M., & Horton-Eddison, M, Corpus Linguistics on the Silk Road(s): The Escrow Example, GDPO Situation Analysis, June, 2017. Available: http://www.swansea.ac.uk/media/EscrowMethodologicalSA110717.pdf

6 Aldridge, J. & Décary-Hétu, D., *Cryptomarkets and The Future Of Illicit Drug Markets*, in EMCDDA. (eds.) *The Internet and Drug Markets*. Luxembourg: Publications Office of the European Union, 2016. P. 25

7 Böhme, R., Christin, N., Edelman, B., & Moore, T., *Bitcoin: Economics, Technology, and Governance*, Journal of Economic Perspectives, Vol. 29, No. 2, Spring, 2015. P. 223

8 Soska, K. & Christin, N., *Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem*, Presented at the 24th USENIX Security Symposium, Washington D.C., 12-14th August, 2015

9 Horton-Eddison, M., *Updating Escrow: demystifying the CDM multisig process*, GDPO Situation Analysis, GDPO, Swansea, July, 2017 Available: http://www.swansea.ac.uk/media/HortonEddisonGDPOMultiSigEscrowSA.pdf

10 Data mirrored by Gwern Branwen (pseudonym), available in raw form here: https://www.gwern.net/DNM%20archives

11 Di Cristofaro, M., & Horton-Eddison, M, Corpus Linguistics on the Silk Road(s): The Escrow Example, GDPO Situation Analysis, June, 2017. Available: http://www.swansea.ac.uk/media/EscrowMethodologicalSA110717.pdf

12 ***'Collocates'*** other words which appear with / alongside the escrow occurrence. Collocates are ranked in order of log-likelihood value, a process which is explained in further detail in the other paper.

13 ***'Occurrences'*** (bits of text) where escrow occurs (con)textually (snippets of posts)

14 For a detailed timeline of these events, see Appendix 1

15 O'Brien, W., *How 2014 Became the Year of Multisig*, Coindesk, 29th December, 2014

APPENDIX 1

Timeline of Events

February, 2011: Silk Road 1.0 (SR1) opens
February, 2012: BIP16 is passed, paving the way for multisig escrow
October, 2013: Silk Road 1.0 (SR1) seized and closed by FBI, loss of at least $3.6million of users' Bitcoin held in escrow
6th November, 2013: Silk Road 2.0 (SR2) opens
13th February, 2014: SR2 Escrow compromised, loss of $2.7million
6th November, 2014: SR2 closed under Operation Onymous

Data Timelines

SR1 data captured on 3rd November, 2013, covers entire SR site on day of seizure, including historic forum entries
SR2 data captured 4th November, 2014, covers entire SR2 from November 2013 to 4th November 2014
SR2a November, 2013 to 12th February, 2014
SR2b 14th February to 6th November, 2014

APPENDIX 2

Multi-Signature Escrow

a) Collocate Findings (SR2)

Despite not appearing at all as a notable collocate of escrow in the SR1 data, multi-signature variants appear prominently in overall SR2 data, providing some of the most often associated collocates: Multi-sig (8th), Multisig (9th), Multi-Signature (47th), and Multisignature (149th). If combined in to one search term, these four variations would appear in the top 3 most associated collocates of escrow in SR2 – compared with nowhere in the top 1000 collocates in SR1 data.

b) Occurrence Examples (SR2a)

"Off the sites is the way to go in my opinion… use native Bitcoin multisig escrow so there is only 1 party in the 3 way escrow. This means that even if the FBI takes servers they can't get any money." *1st December, 2013*

"…simply the fact that the escrow mechanism is multi-sig that reduces the risk of bitcoin loss in the event of **server seizure** … Or is there something more specific about this PHP based market web-site that you can share with us all?" *9th December, 2013*

"AFAIK , SR2 is not using multi-sig escrow or any techniques to prevent hackers (or themselves) from stealing all escrows or balances." *6th December, 2013*

"Do not lose hope there is an ideal solution that will eventually come together: 1. A Tor-based multi-sig escrow site — The ease of using Tor without the risk of being robbed." *9th December, 2013*

"…vendors would post drug listings and independent escrow agents could provide cryptographically secure 2 of 3 multisignature escrow. All we need is bitcoin clients and services that provide easy support for multisignature transactions. You can't DOS a decentralised site since it is split in many parts across many people 's computers, the users themselves. There are **no servers to seize.**" *17th December, 2013*

"This is how we grow as a community …In all seriousness though I think multisig escrow in off market wallets is a good solution." *8th January, 2014*

APPENDIX 3

(de)Decentralised

a) Collocate Findings (SR2)

In relation to escrow, *Centralized* appears at 12th, and *decentralized* is 41st in the SR2 data. Notably, neither word appears in the top 1000 collocates of escrow on SR1. If (de)centralised data is combined with multisig data, they represent the most frequent of any association with escrow in SR2 data.

b) Occurrence Examples (SR2a)

"Escrow could be decentralized too with a similar system or the federated feedback system could allow trust relationships." *10th November, 2013*

"The solution is decentralized Escrow away from the main forum/site. That way when the site is compromised [by LE] the independent escrow agents are not, and still have your money… people should really start thinking about that." *17th November, 2013*

"What we really need is a market place with a decentralized escrow system. That means the escrow funds are distributed across a multitude of trusted accounts." *6th December, 2013*

"Escrow is a great system for protecting buyers in a stable marketplace, but with all this uncertainty it really puts an unfair burden on vendors. Perhaps i2p with decentralized escrow really is the best way to go..." *12th December, 2013*

"You don't need a centralized trusted party to implement escrow, escrow can be decentralized or done away with in general (as it is actually close to worthless). You also don't need a trusted third party to remove malicious users, you can let people ignore users that they don't like." *17th December, 2013*

"a good thing SR got shut down in the end. It reminded us not to be complacent or lightheaded. The void its demise left was filled in little time by numerous uprising contenders. Hell, some are even experimenting using other technologies... Centralized escrow evolved into wallet to wallet transactions, the demise of SR made it very clear that this phenomenon [CDMs] would never stop." *4th February, 2014* cherishde

Swansea University
Prifysgol Abertawe

supported by

OPEN SOCIETY FOUNDATIONS

About the Global Drug Policy Observatory

The Global Drug Policy Observatory aims to promote evidence and human rights based drug policy through the comprehensive and rigorous reporting, monitoring and analysis of policy developments at national and international levels. Acting as a platform from which to reach out to and engage with broad and diverse audiences, the initiative aims to help improve the sophistication and horizons of the current policy debate among the media and elite opinion formers as well as within law enforcement and policy making communities. The Observatory engages in a range of research activities that explore not only the dynamics and implications of existing and emerging policy issues, but also the processes behind policy shifts at various levels of governance.

Global Drug Policy Observatory
Research Institute for Arts and Humanities
Room 201 James Callaghan Building
Swansea University
Singleton Park, Swansea SA2 8PP
Tel: +44 (0)1792 604293
www.swansea.ac.uk/gdpo

GdPo Global Drug Policy Observatory
reportingmonitoringanalysis

@gdpo_swan