GdPO Global Drug Policy Observatory
reportingmonitoringanalysis

Swansea University
Prifysgol Abertawe

GDPO Situation Analysis

July 2017

Updating Escrow:

Demystifying the CDM multisig process

Martin Horton-Eddison[1]

Subject

Until now, the Crypto-Drug Market (CDM) escrow process has been described according to a historic *centralised* escrow system. However, centralised escrow is fast becoming obsolete, with four of the five most popular current CDMs now offering a form of *decentralised* escrow, known as multisignature (multisig). Multisig is therefore fast becoming the industry standard for ameliorating financial risk in CDM transactions. This Situation Analysis is intended to clarify the multisig process. It presents an analysis of the background to the shift toward decentralisation, a description of the new process, and a diagrammatic representation of the multisig escrow model.

Analysis

Despite the anonymity partly afforded by the combined used of TOR[2] and crypto-currencies, early CDMs such as Silk Road were largely conventional websites. They were hosted on geographically physical servers, managed by small teams of tech-savvy administrators, and operated centralised payment systems and escrow services. Silk Road's escrow was designed to mitigate the risks of financial-transactions between vendors and sellers unknown to each other, similar to the systems operated by clearnet ecommerce markets, such as eBay or Aliexpress. Financial transactions were required to be signed off by the administrators of the site, with users' funds held in escrow on the CDM's server until all conditions of the

[1] Researcher and PhD Candidate, Global Drug Policy Observatory

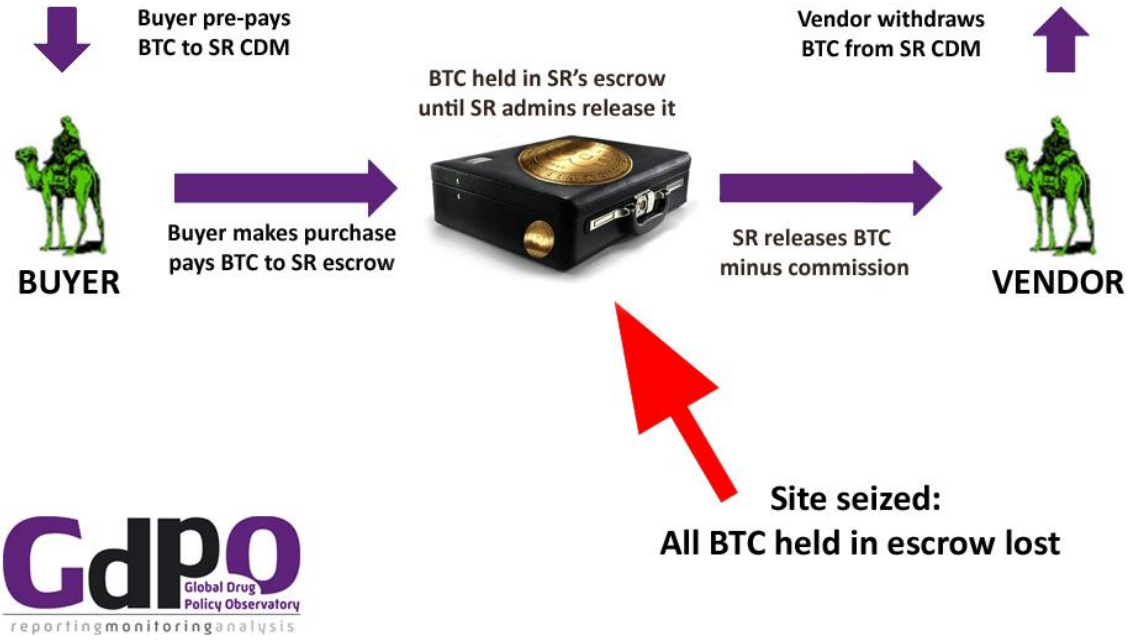
[2] TOR (The Onion Router) Tor is free software and an open network that helps users maintain anonymity online by defending against traffic analysis and obfuscating the user's IP address

transaction were complete.[3] In this way, c*entralised* escrow had the CDM at its heart. During normal operations, this system worked well. Indeed, recent GDPO research[4] shows that on the Silk Road trust in - and adherence to - the centralised escrow system were both very high. However, when the FBI seized the site in October 2013, users lost millions of dollars in Bitcoin (BTC) pending sign-off in in the site's escrow service. And, although many of the site's users migrated to alternative CDMs which also operated centralised escrow systems, it quickly became apparent that users' faith in the DMs' capacity to mitigate *all* risk had been greatly reduced.[5] Specifically, the first whispers of dissatisfaction with the centralised escrow process began within days of Silk Road 2.0's launch in November 2013.[6]

The Silk Road's centralised system had shown itself vulnerable to the effects of 'hard' law enforcement action: site seizure has exposed the core weakness of a system designed for one purpose (trust), but which faced another (security against law enforcement). The same centrality of the CDM which had provided the trust guarantee had also resulted in the loss of funds for both parties. Nevertheless, other CDMs, such as Evolution, Sheep, and (eventually) Silk Road 2.0 continued to operate a centralised escrow model, largely for want of a better alternative. For reference, figure 1.0 is a representation of traditional centralised escrow, as used on Silk Road and others of the era.

Figure 1.0

Silk Road 1.0 Escrow System



[3] For more information on Silk Road's escrow system, see Afilopoaie, A. & Shortis, P, *From Dealer to Doorstep – How Drugs are Sold on the Darknet*, GDPO, Swansea, GFPO Situation Analysis, June, 2015. P. 5

[4] Horton-Eddison, M. & Di Cristofaro, M, *Hard Interventions and Innovation in Crypto-Drug Markets: The escrow example*, GDPO Policy Brief No.11, GDPO, Swansea, June, 2017

[5] *Ibid*.

[6] *Ibid.*

Despite the adoption of centralised escrow by other CDMs, recent research[7] by the GDPO shows that within a month of the FBI's take-down of Silk Road, users of Silk Road 2.0 had begun discussing technical alternatives to the standard model. Outside of the CDM sphere, a February 2012 Bitcoin Improvement Proposal (BIP16) prepared the administrative ground for a solution. BIP16 allowed for the later development of Pay to Script Hash (P2SH) blockchain protocol; the essential technical foundation of multisignature escrow. Multisig achieved technical praxis in August 2013.[8]

As escrow developments progressed outside of the CDM sphere, a series of escrow-related CDM failures occurred. A $40million BTC[9] theft on Sheep in November 2013, followed by a $3.6million BTC scam on Silk Road 2.0 in February 2014, and a $12million BTC administrator-led scam on Evolution[10] in March 2015, all involved abuse of the centrality of the CDM in the escrow process. If the concept of centralised escrow had been wounded by the FBI in October 2013, it was dealt a series of fatal blows by these subsequent scams. Both market and community attitudes turned to multisig for respite.

Multisig Escrow

Decentralised, multisig escrow, as depicted in figure 2.0 (p.4) represents the emerging standard of escrow for many digital transactions, including many 2nd generation CDMs. Indeed, as noted earlier, multisg is now operational on many of the leading CDMs at the time of writing. Multisig decentralizes the financial transaction process, normalising a minimised role for the CDM, and thereby significantly reducing the risk of loss to fraud or law enforcement operations. It removes the historic vulnerabilities of CDM administrators and physical servers from the process. Broadly, multisig permits users (a vendor and a buyer) to enter into the financial transaction element of drug sales whilst retaining both anonymity and trust. The financial process takes place outside of the CDM.

This description is intended to accompany the three stage diagram in figure 2.0.

Stage one represents the purchasing stage. Buyers select from vendor listings on the CDM, just as on SR1 and SR2. However, the CDM's role is now limited to hosting user accounts and the sales listings: no currency is required to be transferred to the CDM's escrow wallet during the purchasing stage. Instead, a multisig wallet is created on a P2SH[11] address, outside of the CDM, on the decentralised blockchain. The multisig wallet has certain pre-conditions attached to it, in this case that two of three public keys[12] are required to finalise a transaction. This is known as 2of3. For sake of simplicity, public keys[13] can be considered as a type of password. In more complex transactions, this 'MofN' sign-off can extend to a maximum of fifteen signatories (Ns). MofN means that the 'power to spend' or finalise a transaction, is not held by any one party alone. This is in contrast to early CDMs, where the power to spend was arbitrarily determined by the CDM administrators through the process of finalising the transaction.

---

[7] Op Cit. Horton-Eddison & Di Cristofaro 2017

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

[9] https://www.deepdotweb.com/2013/11/30/sheep-marketplace-scammed-over-40000000-in-the-biggets-darknet-scam-ever/

[10] Evolution administrator NSWGreat, *Evolution Admins Exit Scamming,* Statement, reddit.com/darknetmarkets, 18th March, 2015. Available: https://tinyurl.com/NSWGreat. Accessed: 05/07/2017

[11] Pay to Script Hash (P2SH) is a blockchain protocol improvement generated as a result of Bitcoin Improvement Proposal (BIP16) approved in February 2012. P2SH enables transactions to be sent to a script hash address (a multisig wallet). To spend crypto-currency sent via P2SH, the recipient/s must provide a script matching the script hash and key/s which match the script requirements.

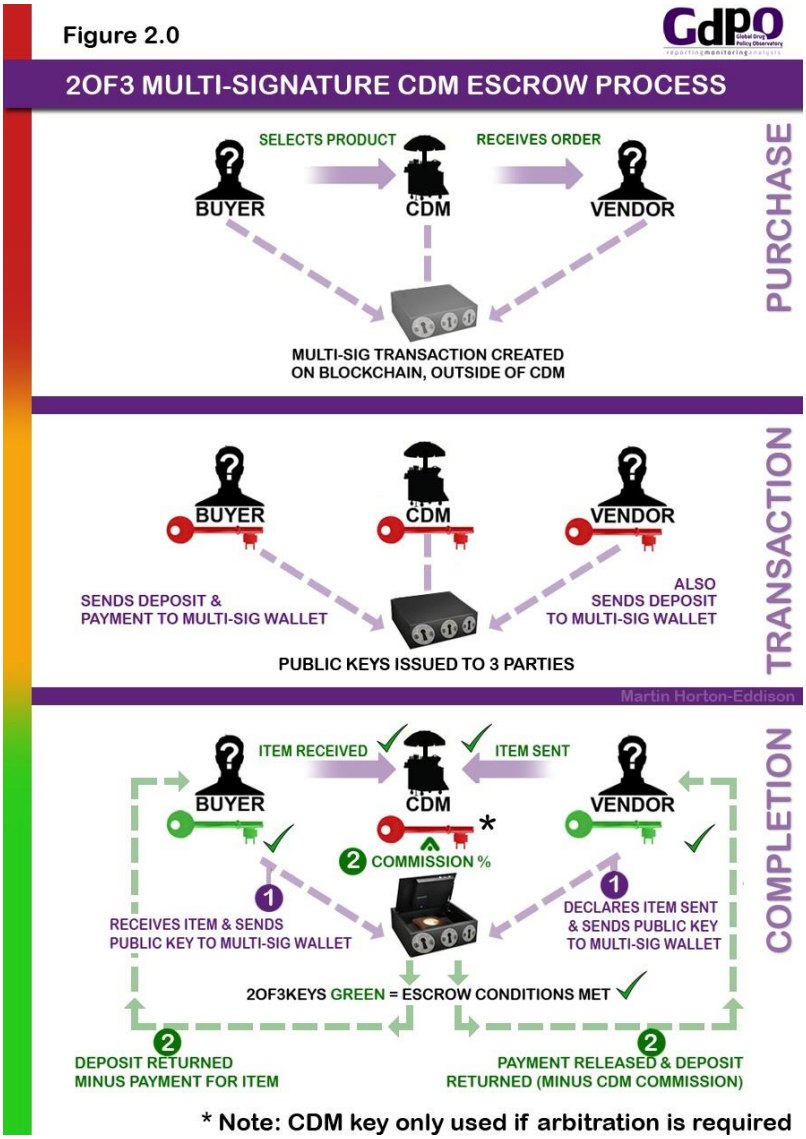
[12] The Private Key is the true 'password' but the Public Key provides proof that a user holds the private key, without having to reveal it.

[13] Although commonly known as public keys, these are formally described as Elliptical Curve Digital Signature Algorithms (ECDSAs)

Stage two is the transaction stage. Both buyer and vendor withdraw funds from their own private crypto-wallets, and deposit these funds in to the multisig wallet on the blockchain. The buyer deposits an amount equivalent to the sale price, plus a refundable deposit. The vendor then matches the buyer's outlay with their own refundable deposit, ensuring that the vendor's financial risk is comparable to the buyer's risk. The exact amounts are transaction and condition specific, and may (but not necessarily) meet or even exceed parity of financial risk. Each party of the transaction is then issued a public key. In figure 2.0, these keys are displayed red.

Stage three is the completion stage. When both the vendor and the buyer are happy that the conditions of the escrow have been met, they input their public keys into the multisig wallet. This occurs when the vendor has declared dispatch of the goods, and the buyer has confirmed receipt of them. As this is a 2of3 escrow, two of the three key holders are required to digitally 'sign' the transaction as complete, and funda are only released when they do so. The diagram shows this as keys turning green. At this stage, any deposit is returned to the buyer, the funds (purchase price) are released onward to the vendor, and the vendor's initial deposit is also returned. A small percentage is also released to the CDM as commission for hosting the original listing. If all works as it should, then this is the CDM's only interaction with the escrow process. Details of the transaction are then broadcast to the internet – i.e. published on the blockchain ledger as verified crypto-currency transfers.

Figure 2.0



Conclusion

Multisig advances several fail-safes over traditional centralised CDM escrow. First, when creating the multisig wallet, a 'seed code' is generated which can be used to recover the location of the wallet from any machine, in case of emergencies such as hardware failure or equipment seizure. Perhaps ironically, the seed code is often written down with paper and pencil. This adds a layer of protection for the buyer and vendor, and both are protected from loss in the event of a site-seizure or other failure of the CDM. No funds are held on the site.

Second, multisig is distributed geographically with no central server, and decentralised administratively, with no centre of authority: it is systemically immune to many of the causes of failure that dogged centralised escrow. If the buyer receives the goods but doesn't enter their public key, the vendor and the CDM can achieve 2of3 by using their keys to release payment. Similarly, if the vendor doesn't enter their key or send the goods, the buyer and the CDM can release payment by entering their keys. Accordingly, no one party in isolation can scam any other without the complicity of a second party. And, since CDMs operate on the twin principals of anonymity and reputation, such an event has a low likelihood. In this sense, multisig escrow allows for the automation of trust. However, the key drawback of decentralised multisig escrow is one of usability. This manifests itself as problematic in two areas. First, the user is required to actually understand the various rudiments of a complitcated process. Second, due to a lack of a Graphical User Interface (GUI) the technical requirements of successful use of multisig may currently be beyond the ability of entry-level CDM users. For now.

Summarily, it seems that Multisig is here to stay, and legacy centralised escrow systems will soon be consigned to the technological ash heap of history. This is partly because Multisig is not exclusive to CDMs, and its utility has been recognised in a number of everyday sectors. Banks and other corporations are investing in mulisi technologies. As they do so, familiarity and usability is likely to improve: an operational user-friendly GUI that simplifies the process for those with only basic IT literacy may signal the start of the next boom in CDM usage in the round.

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_swan

GdPO Global Drug Policy Observatory

reportingmonitoringanalysis