Drop Zone: An Anonymous Peer-To-Peer Local Contraband Marketplace

by Miracle Max
17Q4MX2hmktmpuUKHFuoRmS5MfB5XPbhod

Abstract. Drop Zone is a solution to the problem of restricted sales in censored markets. The proposal is for the design of a protocol and reference client that encodes the location and a brief description of a good onto The Blockchain. Those wishing to purchase the good can search for items within a user-requested radius. Sellers list a good as available within a geographic region, subject to some degree of precision, for the purpose of obfuscating their precise location. Goods are announced next to an expiration, a hashtag, and if space permits, a description. Once a buyer finds a good in a defined relative proximity, a secure communication channel is opened between the parties on the Bitcoin test network ("testnet"). Once negotiations are complete, the buyer sends payment to the seller via the address listed on the Bitcoin mainnet. This spend action establishes reputation for the buyer, and potentially for the seller. Once paid, the seller is to furnish the exact GPS coordinates of the good to the buyer (alongside a small note such as "Check in the crevice of the tree"). When the buyer successfully picks up the item at the specified location, the buyer then issues a receipt with a note by spending flake to the address of the original post. In this way, sellers receive a reputation score. The solution is akin to that of Craigslist.org or Uber, but is distributed and as such provides nearly risk-free terms to contraband sellers, and drastically reduced risk to contraband buyers.

1. Introduction

The diminishment of third party risk is, perhaps, the greatest accomplishment of the modern era. Whereas Gutenberg's press allowed for the affordable dissemination of ideas, The Blockchain allows for the affordable, trustless dissemination of value. Insofar as The Blockchain accomplishes this purpose, it is undeniably a complex, inefficient machine that is good at disintermediating trust. Whether The Blockchain can efficiently accommodate any function outside of that scope with any degree of efficiency remains to be seen. As such, this is a proposal for a framework wherein goods and services whose sale is regularly disrupted by third parties (herein labeled "contraband"), such as Bibles, politically incompatible books[1], vaccines and medicines, or other banned materials, might be delivered to a buyer in such a manner that the risk that is more often borne by suppliers and may be further disintermediated by utilizing the Bitcoin network to deliver contraband to buyers.

In much the same way that Bitcoin allows for two parties who have never met to exchange value, Drop Zone allows users to exchange cash for goods or services without ever meeting. While Nakamoto Consensus via The Blockchain solves the Byzantine General's problem, Drop Zone is much less ambitious in its scope. Still, the projects are closely intertwined, as all modern, formalized contraband marketplaces share the Achilles heel of e-cash systems prior to the introduction of Bitcoin: centralization. And, while proposed solutions to the problem of centralized marketplaces do exist, these projects, to date, are less like decentralized marketplaces[2], and more like distributed marketplaces, thus failing to disintermediate the risk of sellers publicly listing their goods or services. Moreover, most, if not all, of these solutions are larger in scope than a mere distributed protocol meant to accomplish the riskless sale of contraband.

Drop Zone is an elegant protocol for the decentralization of a marketplace, such that derivative applications can be built on top of it to allow users to buy and sell goods without the threat of public scrutiny while sellers will be able to build reputation within the system so that the risk to buyers purchasing from bad actors (defined in this context as those who have an intent outside of the spirit of the agreed upon exchange) can be mitigated as well. Additionally, in an atmosphere with no decentralized marketplace, owners of darknet marketplaces are a single point of failure regarding the privacy and safekeeping of user information. Drop Zone leverages the pseudonymity of the Bitcoin network to allow

users, both buyers and sellers, to be as identifiable or as anonymous as they please. Questions of how anonymous any given user might be will be left to others, considering it is outside of the scope of this proposal.

For messaging that is not contributory to future exchanges, such as communications that are not specific to reputation or that are only needed for the exchange at hand, Drop Zone uses the Bitcoin testnet to avoid polluting The Blockchain.

Note that it is not the intent of this paper to write the reference design. The Drop Zone protocol is more important than the software *per se*, and the multiple client implementations which expand upon this initial guideline should be encouraged. The proposed reference client could be implemented in HTML and JavaScript with signed raw encoded transactions sent via JavaScript to either a user-specified Bitcoind RPC server, or the Blockchain.info API over TOR.

2. Example Usage by a Seller

Bob is new to Drop Zone, and wishes to sell #bibles to his community, which is illegal in his country.

1. Bob opens his Drop Zone client for the first time, which automatically creates an address for Bob on both The Blockchain and the Bitcoin testnet.
2. Bob transfers a small amount of Bitcoin into this address, so that he has enough flake to encode messages into The Blockchain.
3. Bob creates a "seller profile" in his client, which in response creates a DZSLUPDT transaction for his newly funded main-net address. With this profile Bob opts not to choose any alias for himself, but does add the description "I'm a #christian pastor" followed by a link to an imgur picture of Jesus. This description maps to the "d" attribute of the DZSLUPDT transaction, and the generated testnet address's public key maps to the "t" attribute.
4. Not wishing to disclose his exact location, Bob lists his Bibles for sale directly in the center of his city Sinuiju. Bob lists a description of his item, lists it for $10.00 USD, and declares the offer valid for two weeks. The Drop Zone client creates a corresponding DZITCRTE transaction with a d attribute of "Brand new Korean #Bible. Never used. Many available."; a "c" attribute of of "USD"; a "p" attribute of 1000; and an "e" attribute of 2016.
5. Bob waits for customers. The next day, he receives an instant message from a potential customer at his testnet address. He converses with the customer, and discusses the product features. The deal is closed, and the customer wishes to buy three Bibles.
6. Bob creates "Invoice" for the client in the amount of $30, which is valid for one hour. The Drop Zone client creates a corresponding DZINCRTE with a "p" attribute of 300000000 (the conversion rate that hour was $10/BTC) and an "e" attribute of 6.
7. Bob receives payment from the buyer, and hides the Bibles wrapped in a yellow, plastic bag, under a fallen tree in a remote area of town, and notes its GPS coordinates.
8. Bob leaves the Drop Zone, and subsequently messages the buyer and communicates the GPS coordinates, and instructions to look for the yellow bag.
9. The buyer retrieves the item and leaves feedback for Bob in the form of a positive DZINPAID message.

Bob has successfully sold his first contraband and established a small reputation, and can continue servicing his business by responding to other clients who see his listing until its expiration.

3. Example Usage by a Buyer

Alice is an avid user of Drop Zone. In her country, market censorship is a common encumberence. Note that Alice has never bothered to create a profile via the DZBYUPDT message, as she wishes to remain anonymous.

1. Alice opens her Drop Zone client, and searches for unexpired listings which include the tag "#bible" within 80 kilometers, and listed in the last two weeks (2016 blocks).

2. Among the results, she finds one sold by #bob. By scanning his listing address, her Drop Zone client tells her he has no feedback, but he does appears to have the exact item she's looking for.
3. Alice starts a chat with Bob from her Drop Zone client, and negotiates a deal to buy three Bibles.
4. Alice sends Bob the negotiated amount in Bitcoin, to his listing's address on the Main Network ("mainnet"). Alice's Bitcoin is sent from the same address as her public mainnet address. Using these same listing addresses aids the Drop Zone clients in analyzing each actor's reputation for sending and receiving payment.
5. Alice waits a bit for Bob to return the gGPSps coordinates via the message, which he does. Alice proceeds to the Drop Zone, and picks up her package under a tree outside of town.
6. Alice returns home with the Bibles, inspects them, and believes them to be of a high quality.
7. Alice leaves Bob a positive review, in the form of a DZINPAID message, sent to his mainnet Bitcoin address.

4. Bitcoin Mainnet Transaction Encoding

The protocol is designed to require minimal state tracking from clients, with a focus on providing easily indexable transactions for use in performing queries. Herein Drop Zone "transactions" will be labeled "messages" and Bitcoin transactions will be referred to simply as "transactions." The Counterparty[3] metacoin encoding format will serve as a basis reference for data-encoding whenever possible, unless an overriding encoding behavior is defined below. All of the message data will be obfuscated using ARC4 encryption with the same mechanisms as Counterparty. Data may be stored in Counterparty's OP_RETURN, OP_CHECKSIG, or OP_CHECKMULTISIG format. For identification purposes, every Drop Zone transaction's data field will be prefixed by a six character message class encoded in UTF-8. Below are listed all the defined message classes in this initial spec. Each of them begin with 'DZ'. It is the intent for all Drop Zone messages to exist within a single Bitcoin transaction, but as the protocol evolves, it is conceivable that messages could span multiple transactions. Such an encoding is outside the scope of this proposal. Note that unless otherwise denoted, output addresses are to be addressed back to the spender, with the same mechanism as Counterparty's messages. There are some exceptions, which are designed to enable easy indexing by clients. In the case of an item listing, some amount of flake is effectively burned (to be further discussed in depth) for the purpose of providing an index to the geographic location of the listing.

Further details on each message type should be declared based on the above general encoding guidelines. Note that after the message class designation, all values will be inspired by the Bitcoind reference client standards, and will contain subsequent combinations of key-value pairs. After the six-character message class, a variable length string will follow, coupled by a variable-length value (either integer or string, depending on the key). Multiple pairs should follow until the end of the message is reached. Two value types are supported by Drop Zone: variable length integers, and variable length strings. Both encodings should conform to the standards of the Bitcoin reference client[4].

5. Mainnet Drop Zone Message Types

The following message types are intended to serve as a baseline from which the protocol can expand over time. Message keys are delineated as single characters to save space, but the proposed format includes support for larger length keys (aka "attributes")as the protocol evolves. All string characters are valid for use as a key, and all keys are optional unless otherwise specified. Note however, that in many cases attributes (such as testnet communication address and price) are probably required in order to satisfy the execution of a sale between buyer and seller. Each message below is delineated with an indication of who broadcasts the message (either buyer/seller), followed by a colloquial label, and to its right, the six-character message class code. Within each message is a list of defined attributes in the form of

"key/attribute identifier" (data-type): Colloquial description of key/value pair.

Note that transaction output addresses follow the general Counterparty guidelines mentioned above, unless otherwise noted in the message detail below.

Seller Identity Declaration/Update: DZSLUPDT
Seller declarations are required to prefix all item listings, and declare the sender's address as "open for business." However, a seller declaration can occur multiple times after the declaration of an item creation for the purpose of overriding earlier declarations. In the case that multiple seller declarations exist on the same public key, the attributes of the most recent declaration will serve as the relevant declaration.

- "p" (integer): The value of this attribute will be the public key of the seller in the Bitcoin testnet. This testnet address is to be used for all correspondence between the seller and the buyer.
- "a" (string): This is the alias of the seller, meant to identify the seller in a non-unique and colloquial fashion. (i.e., "Satoshi")
- "d" (string): This is the description of the seller, and can contain text and/or URLs of the seller for use in presenting to the buyer.
- "t" (integer): This is enabled for identity transfer, and not intended for use at the time of the address's first declaration. This value is either the new address of the sender, to which all existing earned reputation will transfer, or alternatively, the decimal "0" which indicates the seller is now closed. Any messages after this attribute is declared are no longer valid from this address.

DZSLUPDT Output Address Notes: The output address for this transaction type is "Standard," except for the case of a non-zero "t" attribute that has been defined. In the case that a "t" attribute indicates a new address, the output address must match the address specified in the "t" attribute in order to be valid.

Seller Item Listing Creation: DZITCRTE
The item listing is a special case among message types as it is the only message to make use of the public key in a non-redeemable format. This public key is used to facilitate a simple index by which clients can leverage web APIs for the retrieval of coordinates that match regional search criteria. For the data component of this message, the following attributes are defined:

- "d" (string): This is the description of the item, and can contain text and/or URL of the seller for use in presenting to the buyer. Hashtags are highly encouraged as a mechanism for identifying the item (i.e., #bible).
- "c" (string): The denomination of the price. ISO4217 codes are acceptable, as well as "BTC." Nonce-like constructions should also be supported (i.e., DOGE).
- "p" (integer): The price of the specified item denominated in cents, or satoshis, etc.
- "e" (integer): The expiration time of the item. "Times" are to be indicated in the number of blocks that this listing is available for. Omitting this field indicates no expiration. Note that clients will likely override the seller's preference to list an item for a very long time by restricting the block depth of users' searches.

DZITCRTE Output Address Notes: The output address for this transaction type is a burn output, and deviates from the standard Counterparty format. The output address is a burn address that is prefixed with the magic characters "DZ." What follows are three fixed-size fields: the latitude and longitude of the approximate location (i.e., the center of town), followed by the number of meters within the seller's delivery radius. The latitude and longitude coordinates that follow are in the WGS84 decimal format.

The Latitude field will be a number from 000 to 180 (the degrees of Latitude), followed by 6 digits of precision, with zeros replaced by X. Thus the GPS latitude coordinates -90.000001 will be expressed as XXXXXXXX1 and 89.999999 will be expressed as 89999999.

The Longitude field will be a number from 000 to 360 (the degrees of longitude), followed by 6 digits of precision, with zeros replaced by "X." Thus the GPS longitudinal coordinates -180.000001 will be expressed as XXXXXXXX1 and 179.999999 will be expressed as 179999999.

The delivery radius is encoded in the remaining 8 digits represent the number of meters being serviced by the seller, with X's substituted in place of 0s. Or, alternatively, all Xs for a universal listing (which can be optionally listed by the client).

An example: a listing at WGS84 coordinates: 51.500782, -0.124669 , with a 1 kilometer radius would have the output address of: DZ1415XX782179124669XXXX1XXXZb5saS. In keeping with Bitcoin address standards, the last five characters are the output address's checksum.

Seller Item Listing Update: DZITUPDT

Item updates are designed to update the details of a previously listed item. All of the data fields present in the DZITCRTE message are allowed. The only attribute being defined other than that of the create message is as follows:

- "t" (integer): This attribute is required for this message type. This integer specifies the previously created transaction id being updated.

Note: A DZITUPDT message does not require or support the output address format of the DZITCRTE message.

Note: Setting the "e" attribute to the current block height cancels the availability of the item, and indicates that the item is no longer for sale.

Seller Invoice Creation: DZINCRTE

Invoices are primarily needed to establish a meaningful reputation evaluation of the seller. When a buyer purchases an item from a seller, funds must be sent to the seller following an invoice declaration. Funds received by sellers without a preceding invoice, should not add credit to the seller's reputation.

- "p" (integer): The amount due, denoted in satoshis, which does not include tipping fees.
- "e" (integer): The expiration time of this invoice. "Times" are to be indicated in the number of blocks that this listing is available for. Omitting this field indicates no expiration.

DZINCRTE Output Address Notes:

The output address for this transaction type is addressed to the buyer, and not to the seller, so as to aid with reputation assessment.

Buyer Receipt Acknowledgement: DZINPAID

This message provides an interface primarily for the purchaser of an item to acknowledge receipt of the good and provide feedback on the seller's delivery and product. Multiple DZINPAID messages per DZINCRTE message will be supported, but reputation ramifications will be dependent on the implementor's discretion. Buyers may need to amend a review at some time after its initial issuance. The transaction destination of this message will be addressed to the seller and can contain the following attributes:

- "t" (integer): The transaction ID of the invoice that was generated
- "d" (string): A plaintext feedback string for detailed display on the seller's profile.
- "q": (integer): A score representing the seller's delivery quality. This subjective metric indicates the discretion and quality of arrangement in obscuring and ease of retrieving the dead dropped product. Valid values are between 0 to 8.
- "p" (integer): A score representing the seller's product quality. Valid values are between 0 to 8.
- "c" (integer): A score representing the seller's communication quality. This would be intended to measure literacy and responsiveness. Valid values are between 0 to 8.

Note: It is likely that some sellers will attempt to emulate a "finalize early" strategy that forces buyers to leave reputation prior to receiving product. Subsequent DZINPAID messages could provide additional information after the "early" finalization. This decision might be best reserved until after it is observed how the protocol is used.

Buyer Update/Transfer: DZBYUPDT
Buyer Declarations are optional for buyers, but are available for buyers to declare some form of identity metadata. These can be declared at any time, and in the case that multiple buyer declarations exist on the same public key, the most recent declaration will serve as the relevant declaration.

- “a” (string): This is the alias of the buyer, meant to identify the seller in a non-unique and colloquial fashion (i.e., “Satoshi”).
- “d” (string): This is the description of the buyer, and can contain text and/or URLs.
- "t" (integer): This is enabled for identity transfer, and not intended for use at the time of the addresses first declaration. This value specifies the new address of the buyer, to which all existing earned reputation will transfer. All messages after this attribute is declared are no longer valid from this address.

DZBYUPDT Output Address Notes: The output address for this transaction type is “Standard”, except for the case of a "t" attribute that has been defined. In the case that a “t” attribute indicates a new address, the output address must match the address specified in the “t” attribute in order to be valid.

6. Testnet-based Communication Side-channels

The details on the buyer/seller communications subsystem are being left largely undefined. An encrypted channel should be established over the testnet using the main-net message encoding guidelines whenever applicable. Once established, the buyer's main net public key, and a message signed via its corresponding private key should be transmitted to the seller, to establish the buyer's reputation identity on the seller's Drop Zone client, and to serve as a location to send invoices. After this exchange, a plain text dialog can commence. An additional feature which will enable more efficient conversations , would be the inclusion of a message acknowledgment by both participants upon receipt of each other's messages.

It is recommended that the testnet mempool be used to facilitate lower latency communications. As messages are transitory, and identity is protected via the established PKE channel, Bitcoin block confirmations of the messages are unnecessary. Reference implementations of testnet-based communications already exist and are better described and implemented by other authors[5]. Replay attacks, could be used to attack communications between buyer and seller by way of a denial-of-service, and as such, care should be taken to include a nonce in each communication message.

7. Listing Query Algorithm

It is the intent that all queryable transactions will stem from the identification of an item creation on The Blockchain. These listings will be identified based on the output address of the transaction, and will be discussed further later on in the document. Listing searches, will be performed by examining all blocks created within the specified search time, looking for 'spends' to the burn addresses that comprise the search radius. All such burn addresses will be calculated with the user's current gps coordinates as the origin, and queries should permute through all possible addresses in the search radius. Once retrieved, the listings can be displayed on a map, or in a Craigslist style regional listing. Users can further refine their searches by limiting their queries to whatever terms are in the listing.

8. General Implementation Guidelines

The goal of the project's design should revolve around fast and efficient access by mobile devices, without the need to store The Blockchain, and with the goal of executing queries against web-based api services that have no special knowledge of Drop Zone's functionality. Acceleration for Drop Zone clients, by such services, could be added merely by supporting the use of wildcards when querying public output addresses.

An application specific indexer, such as is available with blockchain.info, will arise that provides useful parsing of the Drop Zone network data in a presentation style similar to that of Craigslist. It is our hope that mobile wallets which already have centralized local marketplace support, such as Airbitz and

Mycelium, route transactions through an anonymized relay, and adopt this proposed protocol over their incumbent solutions.

9. Weaknesses

Sybil Attacks. Such attacks are a distinct possibility within this framework. The identity system as it is described here is rudimentary. Identity, within the Drop Zone protocol would be a cheap to manipulate, and spoofing reputation could even be trivial. Defense against Sybil attacks might be built into applications and third-party analysis tools built on top of Drop Zone, but are not a function endemic to the protocol.

Non-fungible Transactions. Since Drop Zone's transactions are identifiable, miners could begin discriminating against them. This could be resolved by making Drop Zone transactions less identifiable by removing the prefix from the transaction obfuscating the DZITCRTE spend addresses. Such modifications would require the client to perform additional calculations, but would allow unimpeded use of the network. In any case, interaction between miners and Drop Zone transactions is an unknown and should not be pre-optimized.

URL Identifiers are Centralized. URLs in the description fields will likely reference identifiable and centralized locations that are auditable by third-parties. It will always be preferable that TOR-based and/or non-HTTP URLs arrive to host these assets.

Unscrupulous Selling and Asymmetric Risk to Buyers. The Drop Zone protocol has no mechanism for preventing bad acting sellers. The proposed reputation system may mitigate some risk, but cannot remove the risk entirely. The Drop Zone protocol places the risk on the buyers of contraband since their position will be known by the seller. If a bad actor decides to become a seller, it is conceivable that a buyer's anonymity would be compromised.

Unresolved Sales. There are several reasons buyers may not want to acknowledge receipt of a seller's product. Buyers who do not resolve transactions is not directly resolved by the protocol itself, though a possible solution is to implement a separate rating metric for the buyer indicating an unresolved purchases. With this feature, transactions from buyers who do not regularly resolve purchases could be ignored by sellers, though such logistics can be managed in a production wallet and/or GUI presentation.

API Sources. Clients must be careful in selecting an API source for maps. While Google maps may seem like an obvious choice, the risks of presenting coordinates to a map listing service are obvious.

Reputation Selling. In the reference design, it is recommended that sellers be able to sell their reputation so that HD wallets can be supported. There are many potential problems that can arise from the transference of reputation, including, but not limited to reputation scrubbing, in which a buyer will only import good reviews. However, much of this risk is mitigated by the likelihood that good sellers with large amounts of positive reputation will begin messaging from that account in order to exploit the good reputation they acquired.

10. Conclusion

Protocols are agnostic to the actions of participants, and the Drop Zone protocol is no different. Since contraband is often defined by governments, it is important to understand that the purported use case of this protocol is likely to vary widely by location. Moreover, as protocols are expansive and mutable, it is also likely that other yet unconsidered uses will emerge. While governments might define bad actors as those who circumvent the law, this protocol is agnostic to the questions of what is being exchanged and what is allowed to be exchanged and leaves enforcement of local laws to governments.

It is an obvious outcome of the Drop Zone protocol that the enforcement of contraband restrictions will become increasingly difficult. It is likely to shift the burden of legal consequences to

contraband buyers rather than the sellers. Time will answer questions regarding the social outcomes of such a paradigm shift. The simple fact that Drop Zone can be created without the input or risk of government interference is a testament to the strength of Bitcoin's network.

In spite of Bitcoin's strength, it is necessary to acknowledge the added weight to The Blockchain caused by the Drop Zone protocol. Furthermore, as the transactions are identifiable, it is likely that some miners will refuse to process them. The externality of The Blockchain's added weight might be analogized to the chemical dumping of waste into lakes or streams, a form of environmental damage forced upon the participants of Bitcoin. While the burning of funds is necessary in the proposed design of Drop Zone, it is worth noting that the act also amounts to an egalitarian tax: a way for participants to pay for the externality. As for the non-fungible nature of the Drop Zone transactions, miners will likely demand higher fees in order to process them.

Apart from the social consequences of an agnostic, dark market protocol, Drop Zone's most important contribution to contraband markets is its potential to disaggregate dark markets from their participants. While the risk of contraband non-delivery looms over every transaction, just as it always has, the systemic risk presented by the single point of failure of a highly anonymous dark market owner ceases to exist in a model where the listed items, the escrow, and the communications are no longer handled by an unknown server controlled by an unknown actor with unknown motives. In this model, servers querying the protocol act as nothing more than an index of The Blockchain, in the same way that Google is nothing more than an index of the Internet.

The readers of this paper are invited to critique the ideas presented and to ruminate upon their implications.


```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1

mQENBFUTZgcBCADNiHhQnCmcJVvxZbi9BYlhgunEZhgy+sRs+X+3kDOjuqAsEzb9
UJ+OXrGqdG3WzMO1Rn0q7PyytuVCMXhGDhhAUkUe+CAMiMnmVrgsffl54AyPKvl+
PLhWfVjuXfaNx6Z8EwutJb95ZlUtfyHQPcdrG/kqU6Y6+VruFYwWQcoZaJsDYJiw
sfyThUTtxLYoMk6Qd0+v1d+3YBz03nG1OM2d5vun3sSUVBHI+K/r2OFs8AVXVb9e
IhZI/t4hgXMgNk3n8shwo6ryd94O/fzMl2ag9rB6UCqV7aAkdiVds2I28bWTGioD
9O2suj53KRbcAHIvpY+W/koe9On+J6p7nllFABEBAAG0Jk1pcmFjbGUgTWF4IChJ
dCB3b3VsZCB0YWtlIGEgbWlyYWNsZS4piQE4BBMBAgAiBQJVE2YHAhsDBgsJCAcD
AgYVCAIJCgsEFgIDAQIeAQIXgAAKCRDjf1utJkMwyhWgCACKEDb7neTAco0MI1vY
2eAIgDtV/+ts1E9yOoBH2MG2gUnnGT0sAYy7rmqcYq7w3rZo+x5zsvoMAWCn8FyR
cB7wIzHsUwoQ0ebaFJfx9c97DNKpqIxng6MTf/XLH/BBMPeq5XWd8QTltQY6FC6M
Lxv8Fp6OG2Zf2OUwSZXLrgAcsl5YNDNw95X2zNEQ9esCNUM4sC24PtuEe3Zt3Ons
TFr4/JWIK78XtSZGXk5Cm0lS4hPPKixtrgTzKHwIc41bAFC6PjAwXt594Yl57G9j
x0euK3QcO+s0dlr/+Q6dmLOPGBxNB60SYli50DfjDotpqiZ/xEOoI+IcUVELVkrt
A8vquQENBFUTZgcBCADGQts1Vh1GrN8ckCtEs0Z8ip6cTRE3kQwoglcbSgkTyxhb
03vsoOtSjehUWoK293Na8N53t8RDzknAbVaB+H6GoEEiKZmUVTNyaBgfu1CL2sMl
0x4aPG6JdcNOPfqVU8UNaA7fGEdXRsSv7Ub0O9P7fjjnpxVynG+GHjnQb1u37LyA
HaaWoDvyz22Jx/Pzx/rwSPfPdR2kQg331ZMAXv3NfwlPTfgWn000E+X1bUq7R3Oi
qTzapNxlohtzvCSqeYldnNiCpI37FXy33COkBrC/ZZct1cexwXu9S4MbKOejCrIJ
CvX0C/efaua+8S2iICWNkFjKq6uRIvXYByXqsGwXABEBAAGJAR8EGAECAAkFAlUT
ZgcCGwwACgkQ439brSZDMMpiaAf/TQJMriuMefBBAC/c1cr1UwIW44QVM8WzmHwb
hZ6zhDVbLKvFowI6b4ZZCRN73cPwflFL3Pn2QbvvT82zvNxwEDS366z7d5W2Hg9z
Dl14lNnFnk/+hUH4kOot+OJguokMYO4rBnkf2y6sk02L6WR7Xl1bzXd8Vjou3O21
yCtg3sZrzEwOCxoChIaDUsOApvyZn/9PDKS2Tk1Nv/2Ud2UYLBDcklNllCNAQe+W
2ThmI0O1XtXdXzIIwK3vWhWjHuSNbr6Lby+aUmKhMluarJbgR45xahubT9Kz7tZJ
fSie/MBbacKIEIh6pyY+qsfEuiedPM3/pkURZgatd0+O6lXxTQ==
=O9TE
-----END PGP PUBLIC KEY BLOCK-----
```


References

[1] N. Christin, "Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace", https://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12018.pdf, 2012.

[2] D. Zindros, "A pseudonymous trust system for a decentralized anonymous marketplace", https://gist.github.com/dionyziz/e3b296861175e0ebea4b, 2013

[3] http://counterparty.io/

[4] https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_integer, https://en.bitcoin.it/wiki/Protocol_documentation#Variable_length_string

[5] The Royal Fork, “BtcPgp”, : http://www.royalforkblog.com/btc-pgp/