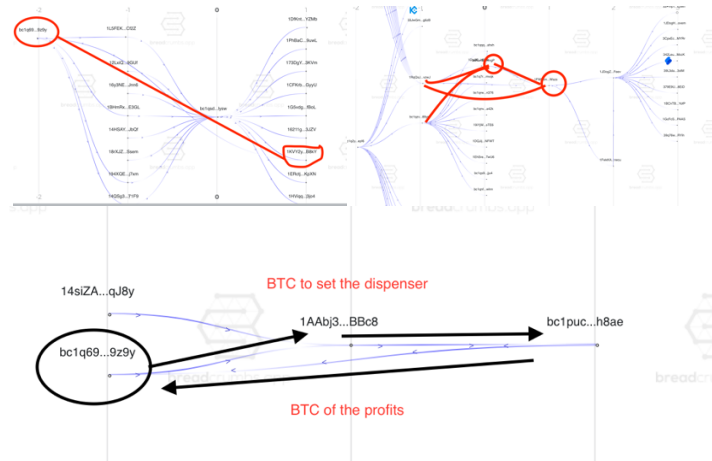


Report: Incident Analysis and Proposed Solutions for Counterparty Dispensers

I. Detected Incidents in Bitcoin Stamps

During the week of May 22nd to May 28th, coinciding with a surge in Bitcoin Stamps growth and purchases, we (Rarestamp team + Mike and Stamphain team) received a flood of notifications from users who had fallen prey to scams.

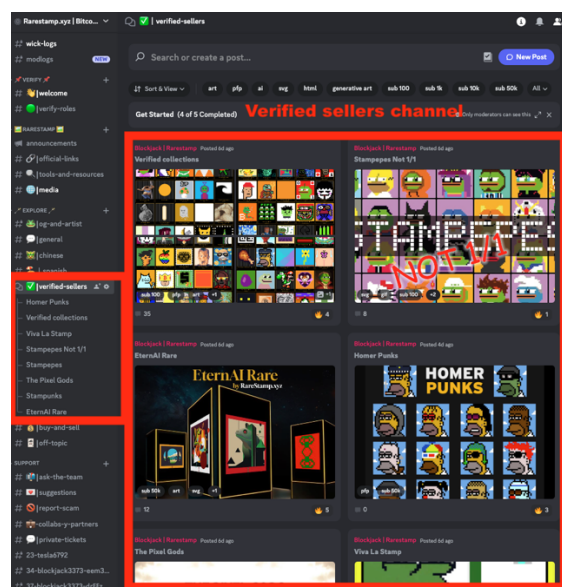
Scammers primarily exploited dispensers for the most expensive and popular collections, closing the dispenser or performing front-run attacks from another of their wallets.



Analysis of some frontrunning attacks cases with breadcrumbs.app

On May 25th, Rarestamp announced two mitigating measures and established a form for reporting scams. The mitigating measures included:

1. Launching a Discord server (<https://discord.gg/BEMq6wSD6x>) with documentation on using dispensers and DEX, as well as risk warnings, and a channel for verified sellers. The intention was not to continually verify sellers through KYC, but as a temporary solution until a better one was found.



2. Initiating development for the integration of Emblem Vault for Bitcoin Stamps. This is currently in development and the MVP is expected to launch in around two weeks.
3. Form for reporting scams <https://forms.gle/hMTL22ybs54LAmAx8>

Despite **21 reported cases**, it is likely that there were many more. Scams have occurred across all price ranges, particularly in the 0.0011 to 0.005 range (Total losses have been reported to be between 0.25 and 0.5BTC in 1 week). The collections with the most reported scams are Homer Punks (due to its high volume and number of assets) and EternAI (due to its higher floor price).

Of the comments received, dispenser closures and front-runs were the most prevalent types of scam. Detailed information, including the responsible wallets, can be found at the end of this document.

II. Proposed Solutions in CIP21 – Dispensers

Counterparty community has a CIP for this issue among other improvements: CIP21 – Dispensers (<https://forums.counterparty.io/t/cip21-dispensers/5488/18>).

The main points of the discussion were(jan 23/2023 to 15 april/2023):

- **loon3** suggested delaying the closing of dispensers, which would prevent operators from closing after receiving payments.
- **jdogresorg** proposed that the delay should only be applicable if there was a pending dispense.
- **JPJA** opposed the idea of delayed closing and proposed a reservation system that would remove the need to trust the seller.
- **sull** suggested dispensers to automatically return BTC to the sender.

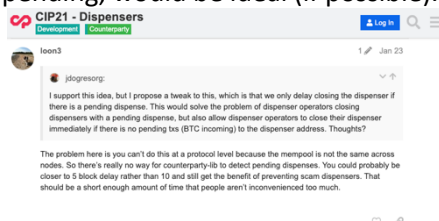
III. My Recommendation (From a Non-Technical guy)

The current dispenser system is broken, affecting many users and **causing a reported losses in 7 days of 6k\$ to 12K\$** an estimated loss of 15-25k\$ over a week. This has resulted in a significant loss of trust in the Xchain platform and has affected the credibility of the entire Bitcoin Stamps project and Rarestamp platform.

Two main problems on the buyer side include 1) cancelled dispensers and 2) front-running by the scammer. On the seller side, refunds due to front-run attacks between users is also a significant issue.

1. Cancelled Dispensers:

- Delaying the closing of dispensers should be a priority. The loss of trust and funds due to this issue outweighs the inconvenience to sellers who set an unintended low price.
- An alternative solution, as proposed by jdogresorg, allowing dispensers to be cancelled early if no transaction is pending, would be ideal (if possible).



2. Front-running:

- There has not been much discussion on front-running issue in the “CIP21- Dispensers”, which affects the most users. If sull's proposal is viable, it would be an ideal solution (dispensers to automatically return BTC to the sender).
- Another potential solution, albeit without technical know-how, could be to create a 1:1 token of XCP that is interchangeable with BTC and recommend using this token for dispenser purchases. By doing this it may be possible to hold this asset until the transactions are confirmed (I do not have the technical knowledge to know if this option is feasible).
- If neither of these solutions is feasible, it is crucial that a viable solution is found as this is as important, if not more important, than addressing the issue of cancelled dispensers.

3. Seller Refunds due to Front-running between Users:

- If a solution to the front-running issue is found, such as Sull's proposal or the alternate solution suggested or any other, this problem would be eliminated, further emphasizing the importance of resolving the front-running issue.

In conclusion, both issues with dispensers cancellations and front-running - should be addressed urgently, given their impact on user trust and the substantial financial losses incurred.

A viable solution must be found and implemented swiftly to restore confidence in the Counterparty project and its associated platforms, and to protect users from further financial losses.

ANSWERS TO THE SCAMS FORM

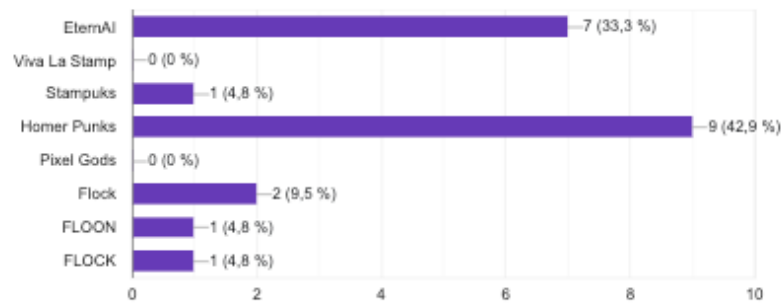
*Check comments section to understand users pain points



Collection where the scam happened | 发生欺诈的收藏

 Copiar

21 respuestas



Wallet of the dispenser | 分发器的钱包

- 1Byn4PtLRNyogupw2FgD9Z6mTL4Qi5eCX1
- bc1qn2w4u7xywtvht7epx5e34qc5y4dy26msq703dn
- bc1q75zcdm9d2dd2hvr5j48uze2fty2x8qkx3p9u
- 14hpLRRH7GqH2MMGiCdxjYovdjLCKvZrpk
- 1CEKktGjAiNeBDTCFUXAzK87HANyXwtGHF
- 16Auj2NbXBgqS7gLgMHT4cgvJRLgw7VgKB
- 1447qh4dpfWNGjNNp4ZFBnTHwmMCvu92tR
- bc1q4wp87v3qznpdm59l6nq4esagnvnaptmrqfpjc8
- 1KpegiakwMWwzvmhEkZUeByYNHJgt8rGhQ
- 14HSAYKRrbYCHqGiWjVhtEkqdcCWJJbQf
- 18rXJZvgqq5APMqc7mzP8wM7cQCMtXSsem
- 1AAbj3iczymTAKTXTR7cUU7Yc8ZmDoBBc8

Link to TX | 交易链接

- 782e1135c68df57ae0fba34336ab97305220208e0acde11fdeb2d781cc41c059
- <https://blockstream.info/tx/9381da0be34e6fcf3964a9790a9abeae9d5c71dd97dbd2b44570aea2e0d64c0e>
- <https://mempool.space/zh/address/bc1qdx7kc5g7dazr5jzwktw3v86lara2a5hscpqyft>
- <https://mempool.space/tx/97cb750ed435beec10d3787c786f551d21a97b0e7782c52d742f95d032e2ac9b>
- <https://mempool.space/tx/8f4cefe80a1f2284da3f79f9ca91c90845781dbcbe16ae74778c69675ee289ed>
- 975f10b664d6dcf353e9aed759a9dc42771b57e1bbe34a18c5b9e43cb03f534f
- 8e33676af0df795bc62d0e79e0e755e6871f1d4b2d05c9c4b68bc4e81f0a18fd
- 937de6b31b84d2671570336c1e08b1592a1faa4134dcf5737dfa08afe1c2635
- c45bdbcecf4241c0653d639b63343a7bbcbcded0b3336c0fd897e0618c06bbe99
- 90f915c49c881c58a0012dadf0f05ea3fa4ef9d20c1c2be989c374e631ffc4b3
- 247ff3a41574b1dcf8ac0ed9b351010b2a0d1004900e26a8679a46c23dc6614
- d62297acfca9bafdf5bdf36ec652dbb78bed616869a231527cbbcff86e9093a7

- a953cbb731ac35099de451d8bf2ef62ee93aa31e9b9e3832c599db38e21405b5
- 1d55d50e34cd0a045696071de0a3595b8810d81e7dbf1c601ab02edd0fe3daa5
- <https://mempool.space/ja/tx/e4668255f5e001a34534ea30bf43ed8348dbef3de3f908e859340bafaf96a659>
- <https://mempool.space/tx/57e5f34ab1341d25f6e00e0b68c3075f6a999588e9830c03b969def04d981197>
- 5f7625fd6262b9413824ba39c4014da120a2518a9224f8ceb4cc7c2cc17ee33d
- 965773769bfc377cf1272d04f63fb8c3e307b800ab08bd850b24147cfe65573c
- 1dfe32956386b8a00ea13a4277ab4ca01e9aa65486bf33d7f777df7cbb23ee65
- ec045e29c96e083455720ddf0d93ef23add017d8f5f6a74616200d94c1f28fde
- <https://blockstream.info/tx/fa7f47204baac1f60450a84ac76097937c1a833d096d2307c12b4d88c6b1dbf5>

Comments or feedback | 评论或反馈

- Show the number of 10 that can be purchased, the seller receives the money, closes the dispenser and transfers the NFT away
- The scammer probably monitors the mempool and knows the purchaser's gas, so no matter how much gas is useless, he will always have more than you. It is not recommended to buy from xchain anymore until the official marketplace is launched. Very bad scam!
- Can you recover your losses?
- I was front run by a transaction. That dispenser was not active for good 1 hour, checked everything and as soon I was ready to transfer, a transaction takes place. and I lose my BTC.
- Looks like the dispenser owner canceled the dispenser.
- This is the matter currently being reported on the ticket. My ID is Tesla#6792. Thank you for investigating this matter.
- Cannot confirm was a scam but I did not receive the NFT, and I have not yet received my 0.02btc back. The dispenser wallet still holds all 0.04btc as of now
- The experience was awful
- tried to buy a Etern AI Rare stamp number 52801
- I purchased STAMP:#52801 from the official website. My transaction got frontran by the scammer. Even though Blackjack was trying to help me with an accelerator website. It still did not workout in my favor. Hoping you guys can do something to get me Unwrecked at least a little bit after this.
- Probably met with a front-run attack. Remittance tx: 939ecafce2bc818cb4cbe9d0af1ad1ee4ad71211b2bead34b7cce8f00feb327e
- spoke to blackjack in discord 'report scam' and super happy you guys are working on incorporating Emblem Vault and for now will def only use verified sellers links... keep up the good work... thank you