

February 26, 2019

VIA ELECTRONIC MAIL

HIT Solution Ltd. d/b/a “HitBTC”

relations@hitbtc.com

legal@hitbtc.com

RE: *Bitcoin Private Listing on HitBTC*

Dear Sir/Madam:

Please be advised that this correspondence has been prepared on behalf of Bitcoin Private (**BTCP**), its developers, contributors, and the Bitcoin Private Community, in response to the unwarranted solicitations and demand for BTCP coins under threat of losing trading support on the HitBTC trade exchange.

In the interests of writing an extensive narrative explaining the facts leading up to HitBTC’s felonious attempt to extort BTCP while simultaneously exposing how and when they defraud Users, what follows is a comprehensive timeline of events that will establish that:

Mar 2, 2018- BTCP launches. As part of its campaign to educate and inform the interest public, it was well publicized that owners of bitcoin (BTC) and ZClassic (ZCL) can get the equivalent of 1:1 ratio of BTCP. To do this, use your private key and transfer it to a new address in readiness for a future coinburn.

May 3, 2018- HitBTC charges BTCP a listing fee in the amount of \$500,000.00 USD, to be paid in bitcoin. In addition to remitting the required listing fee, BTCP also provided HitBTC with a copy of its Whitepaper, which explicitly references the coinburn and its projected date and time of occurrence.

Jan 8, 2019 - Coinburn first mentioned in an article stating it will perform the Coinburn at block number 480,000 on or about Feb 16th, with instructions that BTCP coin holders should move their coin if they hadn’t a block number 480,000 already didn’t.

Jan 27, 2019- Tweet mentioning coinburn at block number 480,000 on or about Feb 16th, further encouraging users to move their coins

Feb 8, 2019- Well publicized article stating the coinburn is due to happen in just over 2 weeks and please transfer coins if you didn't do it as originally instructed

Feb 9, 2019- Countdown on Twitter begins, informing people it's only 7 days till coinburn, move your coins if you didn't before

Feb 10, 2019- HitBTC, in response to an individual question on Twitter asking for instructions and directive as how to keep their BTCP coins held on HitBTC safe from the Coinburn, HitBTC responded on Twitter saying: “There is no need to do anything. Coins in addresses that existed before the creation of BTCP will be made unspendable, but our wallets were created after that time, so they will all be safe.” (see **Exhibit A**)

Feb 11, 2019- Once again, HitBTC responded to public inquiries concerning the safety of HitBTC users’ BTCP coins upon the Coinburn event, HitBTC released a statement via their

public Twitter account stating: “There is no need to do anything. Coins in addresses that existed before the creation of BTCP will be made unspendable, but our wallets were created after that time, so they will all be safe.” (see **Exhibit B**)

Feb 14, 2019 - Countdown on Twitter continues, informing people it's only 2 days till coinburn, move your coins if you didn't before.

Feb 15, 2019 - Countdown on Twitter continues, informing people it's only 1 day till coinburn, move your coins if you didn't before.

Feb 15, 2019 - On the eve of the Coinburn, HitBTC contacts BTCP via Twitter asking for help.

Feb 15, 2019 - Within 30 minutes of receiving the Tweet for help, BTCP developer team members immediately emailed HitBTC asking what issues, if any, could BTCP assist HitBTC in resolving. Quick communication transpired in which HitBTC informed BTCP team members that they were unable to transfer BTCP coins on the exchange from old addresses for "security reasons." Also, HitBTC's request for help to avoid any potential losses which could not yet have occurred (because it was prior to the actual Coinburn), HitBTC requested *compensation* “...**for all of our users BTCP assets which will be affected by the Coinburn.**” (see **Exhibit C** for entire email correspondence)

Feb 15, 2019 - When asked why HitBTC waited until days before the Coinburn to seek the help of BTCP, HitBTC responded as follows:

“Despite the reasons why we haven't done this in advance we cannot let the coins to be burned. Thus we are asking you to compensate our loss that will occur due to your actions.

*We will provide the exact amount of compensation right after the verification of **our users BTCP assets** as BTCP blockchain pass the height of the Coinburning.” (emphasis added)*

Feb 15, 2019 - A support channel on Discord was established in order to provide HitBTC with real-time tech support, as BTCP understood that time was of the essence. Multiple solutions, accompanied with necessary technical information needed to allow HitBTC to transfer BTCP coins, along with tools and examples, were provided to HitBTC— all of which were proven to resolve the purported technological problem of transferring BTCP coins, as complained by HitBTC.

Feb 15, 2019 - HitBTC followed up and informed BTCP that despite the lack of their action, they can't allow the coins to be burned. Within one-hour BTCP provide sound technical assistance. HitBTC are having technical issues making a transfer and again insisting that BTCP agree to compensate them. BTCP informed HitBTC that BTCP was able to help with any technical assistance they needed, however, BTCP would not accommodate HitBTC's demand for compensation. More extensive tech-support was provided to HitBTC, including multiple references to code that was provided for solutions.

Feb 16, 2019 - HitBTC frustratingly expresses it personal opinion that BTCP's ethical Coinburn was “highly controversial and unusual.” HitBTC further claims that funds in their custody may be destroyed and again demanded BTCP provided more solutions. HitBTC proceeded to explain that BTCP's failure to comply with their demand would result in remedial actions on HitBTC's behalf such as taking “all the necessary measures to ensure the guaranteed protection of our custody funds. Those measures might include suspensions of deposits processing, trading suspensions, and complete disintegration.” The total amount of all potentially vulnerable BTCP subject to the Coinburn was 58,920 BTCP (referred to hereinafter as “**Ransom Demand**”). Despite threatening to hold its own Users hostage, BTCP provides HitBTC with two additional test solutions to resolve the issues. No further communication with appointed HitBTC developer “@Foo5eige” and HitBTC was encouraged to discuss the matter internally.

Feb 17, 2019 - Coinburn occurs (block number 480,000 on Feb 16, 2019 10:56:58 PM EST)

Feb 21, 2019 - HitBTC informed BTCP that the help provided was not sufficient, nor timely enough, so as to avoid HitBTC's BTCP coins from being moved prior to the Coinburn. HitBTC alleges to have lost its BTCP holdings due to the coinburn (as expected) and demanded that BTCP compensate those lost coin— stating that the reason they were unable to protect their BTCP from the Coinburn was the fault of BTCP responsibility. HitBTC also alleged that BTCP didn't provide proper solutions. HitBTC then threatened to pull support of BTCP from trading on HitBTC unless we comply with their demand to pay them an amount of BTCP to which they have no legal claim.

Feb 22, 2019 - BTCP again inquires exactly who the custodian of the lost 58,920 BTCP was. No response from HitBTC.

Feb 25, 2019- HitBTC sends the following email to BTCP:

“Hello team,

One of the main goals of HitBTC is to provide safe assets storage in the custody. Custody means a series of organizational procedures and technical instruments which keeps crypto assets safe on the platform.

We are alarmed with uncertain and questionable decision made by BTCP blockchain developers with the idea to burn the coins even if the partners are affected. As there was no clear or constructive response to the previous email we had to stop the deposits. Following steps will be held according to internal schedule.

Still, we believe that it is necessary to promote a constructive and unifying dialogue between us after receiving the compensation of our losses estimated as 58920 BTCP to the following address

[REDACTED]

Waiting for your response as soon as possible.”

After reading the above timeline of events, all of which are supported by documents attached to this correspondence, HitBTC's emails, tweets, activities, and underlying conduct became a cause for concern for BTCP.

To start, HitBTC's February 11, 2019 tweet was particularly strange. As provided above in text, in response to a support question from a HitBTC User, the following tweet was posted:



One cannot help but ask why HitBTC would adamantly inform the public that HitBTC's BTCP User wallets would *not* be negatively affected by the Coinburn, specifically because of the technological impossibility set forth in their response— which is entirely accurate. The only BTCP wallets that would be affected on the HitBTC exchange, or any exchange for that matter, were those wallets which existed *prior to the creation of BTCP* (i.e. coins received from the Bitcoin Segwit blockchain).

To clarify, no BTCP User, on any exchange which supports Bitcoin Private trading, was negatively impacted by the Coinburn. The only BTCP coins in HitBTC's custody that were subject to the Coinburn, based on emails from HitBTC, were BTCP Segwit coins. These BTCP Segwit coins, in that form, could only be obtained if they came directly from claiming BTCP during the original fork, which took place in March 2018 with BTC Segwit. Given the fact that HitBTC, by their own admission and public statement, did not support the BTCP fork for its users, it is *impossible* that the BTCP coins in question could ever possibly be those belonging to HitBTC Users. Furthermore, HitBTC knowingly, intentionally, and deceptively misrepresented their falsified claims in their fraudulent plea for BTCP developer assistance when they stated that it was “**our users BTCP coins**” that were in jeopardy. We now know, clearly, for the aforementioned reasons that was not the case at all.

Instead, the actual problem was that HitBTC publicly stated that its Exchange would NOT support the BTCP fork. However, what HitBTC *actually* meant by that statement, was that HitBTC was not going to support the BTCP fork for anyone other than their own personal benefit. The 58,920 BTCP for which HitBTC repeatedly demanded compensation for, were not those coins lost by its Users during the Coinburn— but rather, BTCP coins secretly held by HitBTC in a BTCP Segwit wallet which they told their Users would not exist. But why? Why forego the generation of revenue that an Exchange like HitBTC would enjoy from supporting this fork for its Users? It is not good practice to hypothecate a criminal actor's motives for engage in such activity, so it is in the interests of both parties to leave that question for a Court to decide during its inevitable investigation of HitBTC's criminal business proclivities.

The actions and conduct of HitBTC as set forth above are unquestionably categorized and defined as “fraud” pursuant to Hong Kong's Theft Ordinance. The Theft Ordinance defines fraud, or fraudulent activity, as follows:

- (1) If any person by any deceit (whether or not the deceit is the sole or main inducement) and with intent to defraud induces another person to commit an act or make an omission, which results either—
 - (a) in benefit to any person other than the second-mentioned person; or
 - (b) in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person,the first-mentioned person commits the offence of fraud and is liable on conviction upon indictment to imprisonment for 14 years.
- (2) For the purposes of subsection (1), a person shall be treated as having an intent to defraud if, at the time when he practises the deceit, he intends that he will by the deceit (whether or not the deceit is the sole or main inducement) induce another person to commit an act or make an omission, which will result in either or both of the consequences referred to in paragraphs (a) and (b) of that subsection.¹

When HitBTC knowingly misrepresented that it would *not* support the BTCP fork to the public— specifically, those members of the public whom expressed direct interest in the status of HitBTC's support of the BTCP fork, as well those currently active Users/customers of HitBTC— it engaged in quintessential conduct falling under the criminal purview of fraud.

However, because the criminal act of “fraud” is so widely defined under Hong Kong laws, for convenience purposes, please allow the following analyses to better describe some of the types of fraud HitBTC engaged in, and how.

¹ Theft Ordinance (Cap. 210. Section 16A “*Fraud*”)

When HitBTC responded to inquiries of its Users whether or not HitBTC Users would receive BTCP at a 1:1 ratio equal to each Users' bitcoin (BTC) holding at the time of the BTCP snapshot, HitBTC (and/or its agents, affiliates, or other authorized personnel) responded via Twitter post as follows:



The *full* link provided in HitBTC's twitter post was "*https://blog.hitbtc.com/system-updates-lot-size-changes/*" which was conveniently taken down shortly after engaging in an extortion-like email correspondence with personnel of BTCP. What's more convenient, is that, prior to HitBTC's timely decision to remove the aforementioned incriminating blog post, a copy thereof was captured for precautionary measures. Of the 40+ digital assets listed on the HitBTC post for which cryptocurrency's were going to be supported by the Exchange, Bitcoin Private was explicitly omitted. By responding to its Users question of fork-support of BTCP, this blog post by HitBTC is statement of response which unequivocally states that fork of BTCP will *not* be supported by the Exchange. (see **Exhibit D** for a true and accurate copy of the afore-mentioned blog page)

However, that was not actually the case. Upon providing repeated public notice to the general public of BTCP intent to schedule a "Coinburn" in the amount of those BTCP coins that were unknowingly distributed as a result of an exploited bug in their Network, HitBTC frantically contacted BTCP's development team via email in an attempt to seek "help" in moving the coins of its "users" to protect their assets. Notwithstanding the fact that HitBTC was given more than sufficient notice (almost six weeks), they opted to seek developer help with an alleged issue less than a week before the Coinburn was scheduled to occur.

By directing interest parties, such as the general public and HitBTC's own Users, to a blog post of HitBTC that was described as the list of the coins, forks, and air drops the exchange would support, HitBTC knowingly engaged in deceptive practices. It is apparent that the BTCP fork was not listed for the public to benefit. In fact, it was purposefully omitted to allow HitBTC to enjoy the windfall of economic benefits received as a direct result of their fraudulent statements.

The aforementioned conduct of HitBTC's business practices in operating their digital asset exchange patently constitutes criminal activity, specifically, obtaining a pecuniary advantage by deception. Section 18 of Hong Kong's "Theft Ordinance" states, in pertinent part, that "Any person [or corporation] by any deception... dishonestly obtains for himself or another any pecuniary advantage shall be guilty of an offence and shall be liable on conviction upon indictment to imprisonment for 10 years."²

² *Idem.* (Cap. 210. Section 18 "Obtaining a pecuniary advantage by deception")

Under the Theft Ordinance, a "deception" is defined as "any deception (whether deliberate or reckless) by words or conduct (whether by any act or omission) as to fact or as to law, including a deception relating to the past, the present or the future and a deception as to the intentions of the person using the deception or any other person."³ Furthermore, the "deception" involved must be effective in securing the pecuniary advantage obtained, however, the fact that the person deceived has suffered no loss as a result of the deception is irrelevant.⁴

Furthermore, pursuant to Section 8 of Hong Kong's "Control of Exemption Clauses Ordinance," HitBTC cannot attempt to shield itself through any of its exemptions clauses against liability when an action arises as a result of HitBTC's own misconduct, including, *inter alia*, breach of contract, fraud, and knowing misrepresentation.⁵

Pursuant to Section 4 of the Misrepresentation Ordinance⁶, any restriction against liability against claims brought by any potential Complainants of HitBTC, is unenforceable against those Complainants who detrimentally relied on HitBTC's fraudulent misrepresentation of fact pertaining to HitBTC's public announcement that it will *not* support the BTCP fork on its exchange— despite knowingly supporting the BTCP fork for its own economic benefit unbeknownst to the general public and actively withheld and concealed from its Users.

When notice of HitBTC's criminal conduct is formally reported to Hong Kong's Securities and Futures Commission and Hong Kong's Monetary Authority, as well as the United States Securities and Exchange Commission, no waiver of liability set forth on HitBTC's homepage will absolve HitBTC, and its individual officers, for its fraudulent and criminal conduct.

The enforceability of the waiver provisions in HitBTC legal disclaimers are questionable at best. Under Hong Kong law, parties are generally free to exclude and limit their liability under a contract subject to the protection to consumers and contracting parties under the Control of Exemption Clauses Ordinance. Under this statute, an exclusion clause may be unenforceable if it is regarded as "unreasonable". (*Lee Yuk Shing v Dianoor International Ltd [2015] HKEC 1294*)

In the event that a formal complaint is filed with the previously referenced enforcement agencies, for the criminally fraudulent activities which HitBTC knowingly and willingly engaged in— Bitcoin Private, the BTCP Community Members, and any and all Users of the HitBTC platform whom currently own, or formally owned, BTCP assets held on the HitBTC Platform— are well within their right to commence a class action lawsuit against HitBTC for damages proximately cause by HitBTC's misconduct. Furthermore, despite HitBTC's purported shield against any such class action lawsuits, as set forth in Section 10.8 of HitBTC's Terms of Service agreement⁷, the enforcement of said waiver against liability is not enforceable.

Therefore, in the interests of good-faith and fair dealing, for the reasons set forth herein, we respectfully request that you immediately cease and desist any and all unwarranted demands for compensation— compensation for which you have no legal right to claim.

³ *Idem.* (Cap. 210. Section 17(4) "Obtaining property by deception")

⁴ Archbold, *Criminal Pleading, Evidence and Practice* (1992 ed, Sweet & Maxwell), at paragraph 17.89.

⁵ Control of Exemption Clauses Ordinance (Cap. 71. Section 8 "Liability arising in contract")

⁶ Misrepresentation Ordinance (Cap. 284. Section 4 "Avoidance of provision excluding liability for misrepresentation")

⁷ "10.8. Whether the dispute is heard in arbitration or in court, you will not commence against HitBTC a class action, class arbitration or representative action or proceeding." <https://hitbtc.com/terms-of-use>

Lastly, should you choose to delist BTCP— as is your right under sole discretionary provisions contained in your Terms of Service— we respectfully request that HitBTC release a public statement explaining to the public and its Users, of that acts that surreptitiously transpired in the days leading up, and following, the Bitcoin Private initial release date.

If you have any further questions or concerns, please feel free to contact me at any time.

Respectfully,

By: 
Peter Hatzipetros, Esq.
Petros Law Group, PC
Legal Counsel for Bitcoin Private

EXHIBIT A

from:hitbtc @bitcoinprivate

Top Latest People Photos Videos News Broadcasts

Search filters · Hide

- From anyone
 - Anywhere
 - All languages
 - Quality filter on
- Advanced search

Who to follow · Refresh · View all

- Cointelegraph** @Cointele...
Follow
 - Ledger** @Ledger
Follow
 - Followed by Daniel Farha
Mizaris @ArisCrypta
Follow
- Find people you know

Trends for you · Change

- ULTRABOOST™**
Retweeted, Reboosted.
Promoted by ads
- #JusticeSmolettHoax**
12.7K Tweets
- Eddie Johnson**
Chicago police say Justice Smolett staged his attack because he was 'dissatisfied with the salary'
- Reggie**
Reggie Fils-Aime to be replaced by Doug Bowser as Nintendo of America president
- Bowser**
A man named Bowser is now the boss of Nintendo of America
- Peter Turk**
Monkeys star Peter Turk has died, reports Washington Post
- Mark Harris**
50.3K Tweets
- Nintendo of America**
54.8K Tweets
- Nick Cafardo**
1.48B Tweets
- #ThursdayThoughts**
158K Tweets

- HIIBCTC** @hitbtc · Feb 15
Replying to @bitcoinprivate
Dear BTCP Team, our Business Development department has tried to reach Jake Brumen & Tim Sulmons via email, but we're yet to receive an answer from you. Looking forward to your answer, you can contact us at relations@hitbtc.com
- HIIBCTC** @hitbtc · Feb 11
Replying to @rultangulo @bitcoinprivate
There's no need to do anything. Coins in addresses that existed before the creation of BTCP will be made unspendable, but our wallets were created after that time, so they will all be safe.
- HIIBCTC** @hitbtc · Jan 5
Replying to @necar31 @bitcoinprivate
Hello! It's hard to say at the moment. Please stay tuned for upcoming updates.
- HIIBCTC** @hitbtc · Feb 18
Replying to @dapatnook @bitcoinprivate
We've contacted the ORME team for more info regarding the swap. Thank you for reaching out, @dapatnook
- HIIBCTC** @hitbtc · Jan 5
Replying to @hold_mybags @bitcoinprivate
All information regarding the support of upcoming forks is being posted in our twitter and blog. Please stay tuned for upcoming updates!
- HIIBCTC** @hitbtc · Jan 6
Replying to @necar31 @bitcoinprivate
No, you can freely operate your BTCP coins. Transfers and withdrawals remain available.
- HIIBCTC** @hitbtc · Jan 28
Replying to @Crypto_Giant199 @thasoty2000 and 2 others
Sorry to hear such opinion. Please note that transaction processing time is determined by the network speed, not by us.
- HIIBCTC** @hitbtc · 26 Dec 2018
Replying to @Nikkidoudeman @bitcoinprivate
The minimum trading lot is designed due to the overall convenience. It also helps to maintain the stability of trading operations. We aren't sure that we have got you right about BTCP. Could you kindly clarify what's wrong?
- HIIBCTC** @hitbtc · 28 Oct 2018
Replying to @hold_mybags @bitcoinprivate
It is hard to say at the moment, unfortunately. We will make an announcement on our Twitter if this happens. Stay tuned!
- HIIBCTC** @hitbtc · 8 Nov 2018
Replying to @bitcoinprivate, @CryptoCoinsNews and 8 others
Hey @bitcoinprivate! Looks like someone is impersonating your account here.
- HIIBCTC** @hitbtc · Feb 18
Replying to @bitcoinprivate
Our team was in the middle of the conversation with Tim, but he stopped responding for some reason. This inquiry is urgent and needs to be addressed as soon as possible - looking forward to your reply.
- HIIBCTC** @hitbtc · Jan 28
Replying to @thaib2000 @bitcoinprivate @TradeSatoshi
Have you contacted our support team regarding the issue? support.hitbtc.com/hc/en-us
You can share the ticket number right here.
- HIIBCTC** @hitbtc · 30 Dec 2018
Replying to @hold_mybags @bitcoinprivate
We usually post updates regarding the airdrops on our social media and/or blog. Please stay tuned for more information on the matter.
- HIIBCTC** @hitbtc · 30 Nov 2018
Replying to @CryptoEza @jaysface @bitcoinprivate
Confirmation amount is calculated upon the current state of BTCP network to ensure our users' maximum security. Thank you for understanding.
- HIIBCTC** @hitbtc · 7 Nov 2018
Replying to @88Crypto88 @hold_mybags @bitcoinprivate
Watch us here. If there will be an update regarding this - we will let our community know.
- HIIBCTC** @hitbtc · 31 Oct 2018
Replying to @cryptoddmu @hold_mybags and 2 others
Please follow our social media and Blog for the updates: we post all information there!
- HIIBCTC** @hitbtc · Feb 14
Replying to @CryptoHDL_Amit @bitcoinprivate
You do not need to do anything. Coins in addresses that existed before the creation of BTCP will be made unspendable - our wallets were created after that time, so the developers assured us they will be safe.
- HIIBCTC** @hitbtc · Jan 7
Replying to @Huntington_HodL @Mikhael5527473 @bitcoinprivate
All the information regarding the support of certain forks and airdrops is being posted on our twitter and blog. Please stay tuned for upcoming updates!

EXHIBIT B



[\[Redacted\]](#) · Feb 10

[@hitbtc](#) hi. I saw the btcp tweet about the coin burn in 7 days. I got btcp in hitbtc. Please advise what should I do?



HitBTC
[@hitbtc](#)

Follow

Replying to [\[Redacted\]](#)

There's no need to do anything. Coins in addresses that existed before the creation of BTCp will be made unspendable, but our wallets were created after that time, so they will all be safe.

12:11 PM - 11 Feb 2019



EXHIBIT C



Peter Hatzipetros <peterh@petroslawgroup.com>

Re: Re Bitcoin Private?

10 messages

Tim Sulmone <tim@btcprivate.org>

Fri, Feb 15, 2019 at 6:56 PM

To: Relations HitBTC <relations@hitbtc.com>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, peterh@petroslawgroup.com

We are more than willing to help in any technical regard, however regarding compensation, we will be unable to provide this. We recommend taking the action we have provided to achieve moving your coins before the burn to prevent loss.

Regarding the tx issue:

see sendrawtransaction or sendtoaddress, not z_sendmany

<https://github.com/BTCPrivate/BitcoinPrivate/blob/b27c72274922eec86f301c2d1a7078dc038cfad6/src/script/standard.h#L40>

need all three; SCRIPT_VERIFY_P2SH, SCRIPT_VERIFY_CHECKLOCKTIMEVERIFY, SCRIPT_VERIFY_FORKID;

<https://github.com/BTCPrivate/BitcoinPrivate/commit/54f102248b183618ed7bd198c995232c89dc3152#diff-7ec3c68a81eff79b6ca22ac1f1eabbaL1591>

<https://github.com/BTCPrivate/BitcoinPrivate/blob/master/src/script/standard.h#L64> this line is the root of the return error

If assistance is still needed, an example tx that you are trying to build would be helpful so we can look through errors in formatting.

Thank you,

Tim Sulmone

P.S. I have CC'ed in Peter whom is our Legal Council.

On Fri, Feb 15, 2019 at 4:47 PM Relations HitBTC <relations@hitbtc.com> wrote:

Dear Tim, thank you for the reply!

We do appreciate your help with the situation however we still want to have your full guarantee regarding providing the compensation for all of our users BTCP assets which will be affected by the coin burn.

Please see the comment from our dev team below:

We implemented forkid params, but resulting transaction still can't be pushed with sendrawtransaction and results in {"result":null,"error":{"code":-26,"message":"64: non-mandatory-script-verify-flag (No error)","id":null}} we've tried to look for clues in wallet code, but it uses z_sendmany, which doesn't even operate with bitcoin utxos.

Best regards,

Janna Kovich

HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

On Fri, 15 Feb 2019 at 23:34, Tim Sulmone <tim@btcprivate.org> wrote:

Hello, I had a chance to speak with one of our main developers and was able to get the information requested:

sig:

<https://github.com/BTCPrivate/BitcoinPrivate/blob/b27c72274922eec86f301c2d1a7078dc038cfad6/src/script/sign.cpp#L331>

sighash:

needs to be | SIGHASH_FORKID (0x40)

SignatureHash uses FORKID_IN_USE << 8 appended to the end aka FORKID_BTCP (42)

<https://github.com/BTCPrivate/BitcoinPrivate/blob/b27c72274922eec86f301c2d1a7078dc038cfad6/src/script/interpreter.cpp#L1111>

Full script evaluation:

<https://github.com/BTCPrivate/BitcoinPrivate/blob/b27c72274922eec86f301c2d1a7078dc038cfad6/src/script/interpreter.cpp#L252>

2a00 is 42 << 8

The examples in <https://github.com/BTCPrivate/BitcoinPrivate/pull/77> should reflect the right results

witness part goes to scriptSig instead, scriptPubKey remains as expected with 0P_0 start

Example Segwit Claim/Spend with blockexplorer links: <https://bitcointalk.org/index.php?topic=2675257.msg34531713#msg34531713>

There are also relevant third-party tools for accomplishing such tasks, such as:

<https://github.com/Ayms/bitcoin-transactions>

https://github.com/yngve/bitcoin_fork_claimer

If you have any further questions, please feel free to ask :-)

Sincerely,

Tim Sulmone

On Fri, Feb 15, 2019 at 2:26 PM Relations HitBTC <relations@hitbtc.com> wrote:

Matt, TIm,

as Jake is not a part of the team anymore I will delete him from the conversation.

Despite the reasons why we haven't done this in advance we cannot let the coins to be burned. Thus we are asking you to compensate our loss that will occur due to your actions.

We will provide the exact amount of compensation right after the verification of our users BTCP assets as BTCP blockchain pass the height of the coin burning.

Best regards,

Janna Kovich

HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

On Fri, 15 Feb 2019 at 21:03, Jake Brutman <jake@btcprivate.org> wrote:

Janna,

I'm no longer a part of the BTCP contribution team. Your best bet is talking to the developers. But as far as I can see the issue is that you're trying to claim your own coins and not that of users, correct?

The white paper clearly specified this action would happen around now. Is there a reason you waited until the last minute to address it?

Jake

On Fri, Feb 15, 2019 at 12:00 PM Relations HitBTC <relations@hitbtc.com> wrote:

Jake,

please see the conversation below.
We will appreciate your help with answer on the last question.

Best regards,
Janna Kovich
[HitBTC](#) business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

----- Forwarded message -----

From: **Relations HitBTC** <relations@hitbtc.com>
Date: Fri, 15 Feb 2019 at 18:37
Subject: Re: Re Bitcoin Private?
To: Matt Pass <matt.pass@btcprivate.org>
Cc: Tim Sulmone <tim@btcprivate.org>

Thank you.

We're trying to send segwit following <https://github.com/BTCPrivate/BitcoinPrivate/pull/77>
the only problem is signature:

- 1) how is signature and sigHash are calculated?
- 2) whats the correct sigScript for segwit ? <sig> <pubkey> <segWit address (op_0 pubKeyHash)> ?

Best regards,
Janna Kovich

HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

On Fri, 15 Feb 2019 at 18:22, Matt Pass <matt.pass@btcprivate.org> wrote:

Hi Janna

It may be a good idea for you to talk to our team in this Discord channel we have arranged for you:

<https://discord.gg/MX7Pqv>

On Fri, Feb 15, 2019 at 3:02 PM Relations HitBTC <relations@hitbtc.com> wrote:

Matt,

Due to security reasons we can't have an access to this addresses right now so we are unable to make the transfers at proper time.

We need an acknowledge that even if we can't transfer the coins we will receive a compensation equals the number of the coins we have on our addresses at the moment.

Best regards,
Janna Kovich
HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

On Fri, 15 Feb 2019 at 17:55, Matt Pass <matt.pass@btcprivate.org> wrote:

Hi Janna

We may be able to advise best if we can understand the security reasons, perhaps it could help us. Everything you tell us is of course in the strictest confidence.

A transfer must be present on the BTCP blockchain to avoid coins being burned.

I have included Tim into this conversation to help.

Matt Pass
Bitcoin Private.

On Fri, Feb 15, 2019 at 2:48 PM Relations HitBTC <relations@hitbtc.com> wrote:
Hi Matt,

We can't transfer BTCP from the old addresses due to security reasons. We are kindly asking you to assist us with resolving this issue without burning the coins.

Best regards,
Janna Kovich
[HitBTC](#) business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

On Fri, 15 Feb 2019 at 17:21, Matt Pass <matt.pass@btcprivate.org> wrote:
Hi Janna

You're unable to transfer BTCP on old addresses to new addresses? What is the technical issue you're facing and do you have the private keys?

If so, you should be able to transfer them OK?

Matt Pass
Bitcoin Private

On Fri, Feb 15, 2019 at 2:10 PM Relations HitBTC <relations@hitbtc.com> wrote:
Dear Matt,
Thank you for the prompt response!

We have an urgent question to your team but unfortunately we can't reach Jake or Tim by the email (obviously because they are not working anymore)

We have BTCP coins on the old addresses and we can't transfer them to another ones due to technical problems. How we can save the coins without burning them? Could you advise the best solution?

Best regards,
Janna Kovich
[HitBTC](#) business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

On Fri, 15 Feb 2019 at 17:05, Matt Pass <matt.pass@btcprivate.org> wrote:
Hi there

We've noticed you tried to contact us via Twitter (re the message: "**@bitcoinprivate Dear BTCP Team, our Business Development department has tried to reach Jake Brutman & Tim Sulmone via email, but we're yet to receive an answer from you. Looking forward to your answer, you can contact us at relations@hitbtc.com**")

Jake is no longer working for Bitcoin Private. I'm a web developer but can hopefully answer your enquiry or will pass it onto a blockchain dev?

Please let me know how we can help and we'll get back to you very soon.

Thanks
Matt Pass
Bitcoin Private

--
Regards,
Jacob Brutman
Operations Lead
Bitcoin Private

Relations HitBTC <relations@hitbtc.com>

Sat, Feb 16, 2019 at 5:03 AM

To: Tim Sulmone <tim@btcprivate.org>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, peterh@petroslawgroup.com

Tim,
Thank you for assistance!
We have one more question from our dev team:

What is the correct scriptPubKey to sign to spend segwit utxo ? Which is p2sh-p2wpkh.

we've tried signing p2sh, p2kh, still no results.

and scriptSig <signature> <pubkey> <0014 hash160>

hex transaction example: 0100000001a490ace17e83ae6880625f6d8336a44e2444a718623348c537

d784a1f6ee7376000000082483045022100cd47eeaa65aa0c96d1274e4cb5401b8e0c1ae7e247abd520abfe73

5cc5d36f9d0220329543479c66c4a6d0cb51074f9aadfac50735f7862a11883e47e8e8cfc6dfb141210317aadf

73b5a8bb152d3cd6ba4c729704e99fcf752d3f42bae20adaae8bf0b767160014030da09965cb1c17b1736f00ef

c6252d5c7e66a9ffffff016048980000000001976a9145081c5e50e249a654008b63eac42094bc934183188ac00000000

Best regards,
Janna Kovich
HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read

any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

[Quoted text hidden]

Relations HitBTC <relations@hitbtc.com>

Sat, Feb 16, 2019 at 6:21 AM

To: Tim Sulmone <tim@btcprivate.org>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, peterh@petroslawgroup.com

Dear Tim,

The discord channel you mentioned in the email is not working unfortunately - <https://discord.gg/MX7Pqv>

Can you provide the new one or do you have a telegram account to chat with your dev team for speeding up the process of resolving the issues?

Thank you!

Best regards,
Janna Kovich
HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

[Quoted text hidden]

Tim Sulmone <tim@btcprivate.org>

Sat, Feb 16, 2019 at 10:00 AM

To: Relations HitBTC <relations@hitbtc.com>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, peterh@petroslawgroup.com

Hello,

witness: (n/a)

scriptSig: <sig> <pubkey> <OP_0 <hash160(<pubkey>)>>

scriptPubKey: OP_HASH160 <hash160(OP_0 <hash160(<pubkey>)>)> OP_EQUAL

Transactions are hashed with the OLD (pre-segwit) hashing scheme.

I hope that help clear up any confusion.

Thanks,
Tim Sulmone

P.S. The discord link worked, we saw username "Foo5iege" join asking about segwit utxo's, but unfortunately they left the discord before anyone could assign a role or respond. (most of us are American timezone). Feel free to rejoin :-)

<https://discord.gg/3SeNztB>
[Quoted text hidden]

Tim Sulmone <tim@btcprivate.org>
To: Relations HitBTC <relations@hitbtc.com>
Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, peterh@petroslawgroup.com

Sat, Feb 16, 2019 at 5:24 PM

Hello,

We had a chance to speak to "Foo5iege" in discord. Here is a compilation of the technical support solutions surrounding this issue.

full RPC example:

```
PRIV_KEY=L5fQCL1H7H5Pa6NxcMGXh3gN7StU7V2giJ5GYHbg7LbZb6HWKmdF
P2SH_P2WPKH_ADDRESS=bxefaFLhLgHoNBmdpJcGsz9XTsxS75UntSk
P2SH_P2WPKH_PUBKEY_HEX=a9142272205f88e0478433e3ae8e94d7280d659e331887
REDEEM_SCRIPT=0014c7c61797bb93fbbab5bf2a0ed3e4f1e883c7fa76
./btcp-cli -regtest generate 101
./btcp-cli -regtest importprivkey $PRIV_KEY
TXID_FROM=`./btcp-cli -regtest sendtoaddress $P2SH_P2WPKH_ADDRESS 1`
./btcp-cli -regtest generate 1
T0=`./btcp-cli -regtest getnewaddress`
RAW_TX=`./btcp-cli -regtest createrawtransaction [{"txid":"$TXID_FROM",
vout":0}]' '{"'$T0':0.9999}' `
SIGNED_TX=`./btcp-cli -regtest signrawtransaction $RAW_TX [{"txid":"$TXID_FROM",
"vout":0, "scriptPubKey":"$P2SH_P2WPKH_PUBKEY_HEX", "redeemScript":"$REDEEM_
SCRIPT"}]' '{"'$PRIV_KEY'}' | grep hex | sed -E 's/.*"(.*)",.*\/\1/'`
./btcp-cli -regtest sendrawtransaction $SIGNED_TX
./btcp-cli -regtest generate 1
```

Test case:

```
BOOST_AUTO_TEST_CASE(segwitspend_shwpkh)
{
    CKey key;
    key.MakeNewKey(true);
    CScript unwrappedPubKey;
    unwrappedPubKey << OP_DUP << OP_HASH160 << ToByteVector(key.GetPubKey().GetID()) <<
    OP_EQUALVERIFY << OP_CHECKSIG;
    CScript segwitPubKey = GetScriptForWitness(unwrappedPubKey);
    CScript p2shsegwitPubKey = GetScriptForDestination(CScriptID(segwitPubKey));
    CScript p2shsegwitScriptSig;
    p2shsegwitScriptSig << Serialize(segwitPubKey);
    CMutableTransaction txFrom;
    txFrom.vout.resize(1);
    txFrom.vout[0].scriptPubKey = p2shsegwitPubKey;
    CMutableTransaction txTo;
    txTo.vin.resize(1);
    txTo.vin[0].prevout.n = 0;
    txTo.vin[0].prevout.hash = txFrom.GetHash();
    txTo.vout.resize(1);
    txTo.vout[0].nValue = 1;
    auto sighash_flags = SIGHASH_ALL | SIGHASH_FORKID;
    uint256 hash = SignatureHash(unwrappedPubKey, txTo, 0, sighash_flags,
    FORKID_IN_USE);

    std::vector<unsigned char> vchSig;
    key.Sign(hash, vchSig, 0);
    vchSig.push_back(static_cast<unsigned char>(sighash_flags));
    txTo.vin[0].scriptSig << vchSig << ToByteVector(key.GetPubKey());
    txTo.vin[0].scriptSig += p2shsegwitScriptSig;
    ScriptError err;
    BOOST_CHECK(VerifyScript(txTo.vin[0].scriptSig, txFrom.vout[0].scriptPubKey,
```

```

SCRIPT_VERIFY_P2SH | SCRIPT_VERIFY_WITNESS | SCRIPT_VERIFY_FORKID,
MutableTransactionSignatureChecker(&txTo, 0), &err));
std::cout << "Script error string: " << ScriptErrorString(err) << std::endl;
BOOST_CHECK(VerifyScript(txTo.vin[0].scriptSig, txFrom.vout[0].scriptPubKey,
MANDATORY_SCRIPT_VERIFY_FLAGS,
MutableTransactionSignatureChecker(&txTo, 0), &err));
std::cout << "Script error string: " << ScriptErrorString(err) << std::endl;
BOOST_CHECK(VerifyScript(txTo.vin[0].scriptSig, txFrom.vout[0].scriptPubKey,
STANDARD_SCRIPT_VERIFY_FLAGS,
MutableTransactionSignatureChecker(&txTo, 0), &err));
std::cout << "Script error string: " << ScriptErrorString(err) << std::endl;
}

```

```

./src/test/test_bitcoin --run_test=script_P2SH_tests/segwitspend_shwpkh
Running 1 test case...
Script error string: No error
Script error string: No error
Script error string: No error

```

*** No errors detected

Can put this in main.cpp to help give a more informative error message(if issue persists)

```

--- a/src/main.cpp
+++ b/src/main.cpp
@@ -1774,6 +1774,7 @@ bool ContextualCheckInputs(const CTransaction& tx,
CValidationState &state, cons
pvChecks->push_back(CScriptCheck());
check.swap(pvChecks->back());
} else if (!check()) {
+ const char * origError = ScriptErrorString(check.GetScriptError());
if (flags & STANDARD_NOT_MANDATORY_VERIFY_FLAGS) {
// Check whether the failure was caused by a
// non-mandatory script verification check, such as
@@ -1784,7 +1785,7 @@ bool ContextualCheckInputs(const CTransaction& tx,
CValidationState &state, cons
CScriptCheck check(*coins, tx, i,
flags & ~STANDARD_NOT_MANDATORY_VERIFY_FLAGS, cacheStore);
if (check())
- return state.Invalid(false, REJECT_NONSTANDARD, sprintf("non-mandatory-script-
verify-flag (%s)", ScriptErrorString(check.GetScriptError())));
+ return state.Invalid(false, REJECT_NONSTANDARD, sprintf("non-mandatory-script-
verify-flag (%s)", origError));
}
// Failures of other flags indicate a transaction that is
// invalid in new blocks, e.g. a invalid P2SH. We DoS ban

```

Thanks,
Tim Sulmone

Relations HitBTC <relations@hitbtc.com>

Sat, Feb 16, 2019 at 5:41 PM

To: Tim Sulmone <tim@btcprivate.org>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, Peter Hatzipetros <peterh@petroslawgroup.com>

Dear team,

Thank you very much for your technical support.

We appreciate your ambitions in creating new blockchain technologies. Despite that, your decision to destroy BTCP user funds is highly controversial and unusual.

If you decide to do it, part of funds in our custody will be destroyed. We kindly ask you to provide a solution to eliminate the risk of our custody of losing assets.

Our top priority is the safety of funds in our custody. According to our policy, we cannot work with systems causing risks of losses against our will. In case we would not have a solution and will lose any funds, we will have to fix our losses and take all the necessary measures to ensure the guaranteed protection of our custody funds. Those measures might include suspensions of deposits processing, trading suspensions, and complete disintegration.

We are kindly asking you to provide a plan to eliminate the risks of losses in our custody as soon as possible.

We estimate our potential losses from your actions as 58920 BTCP.

Best regards,

Janna Kovich

HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

[Quoted text hidden]

Tim Sulmone <tim@btcprivate.org>

Sat, Feb 16, 2019 at 6:35 PM

To: Relations HitBTC <relations@hitbtc.com>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, Peter Hatzipetros <peterh@petroslawgroup.com>

We provided "Foo5iege" with two test solutions to resolve the issues you brought to our attention. TO reiterate, we still have not heard back from Foo5iege or anyone else on your development team. We urge you to discuss this matter internally, as time is of the essence.

Sincerely,

Tim Sulmone

[Quoted text hidden]

Relations HitBTC <relations@hitbtc.com>

Thu, Feb 21, 2019 at 6:42 AM

To: Tim Sulmone <tim@btcprivate.org>

Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, Peter Hatzipetros <peterh@petroslawgroup.com>

Dear team,

Your support and help in resolving all the technical issues are highly appreciated but, unfortunately, it wasn't as efficient and prompt as it has to be. Due to a coin burn, carried out by your team, our custody has lost control over the BTCP

assets.

We are kindly proposing you to compensate custody losses until February 23th 00:00 UTC, as this coin burn was both your decision and responsibility and you didn't provide our team with the proper solutions. If we won't have an agreement until that time, we will have to suspend deposits and trading activity with the following disintegration of BTCP due to our custody policy. We estimate our losses as 58920 BTCP.

Best regards,
Janna Kovich
HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

[Quoted text hidden]

Tim Sulmone <tim@btcprivate.org> Thu, Feb 21, 2019 at 1:53 PM
To: Relations HitBTC <relations@hitbtc.com>
Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, Peter Hatzipetros <peterh@petroslawgroup.com>

Hello,
Thank you for your message. Can you please elaborate further on precisely whose custody of 58,920 BTCP was "lost" during the coinburn?

Sincerely,
Tim Sulmone
[Quoted text hidden]

Relations HitBTC <relations@hitbtc.com> Mon, Feb 25, 2019 at 1:12 PM
To: Tim Sulmone <tim@btcprivate.org>
Cc: Matt Pass <matt.pass@btcprivate.org>, Tim Novak <tn@hitbtc.com>, Peter Hatzipetros <peterh@petroslawgroup.com>

Hello team,

One of the main goals of HitBTC is to provide safe assets storage in the custody. Custody means a series of organizational procedures and technical instruments which keeps crypto assets safe on the platform.

We are alarmed with uncertain and questionable decision made by BTCP blockchain developers with the idea to burn the coins even if the partners are affected. As there was no clear or constructive response to the previous email we had to stop the deposits. Following steps will be held according to internal schedule.

Still, we believe that it is necessary to promote a constructive and unifying dialogue between us after receiving the compensation of our losses estimated as 58920 BTCP to the following address b16ZWYbZijKRQCnjoNo9teDvxK3HCcX71i7

Waiting for your response as soon as possible.

Best regards,
Janna Kovich
HitBTC business development



CONFIDENTIALITY NOTICE: This transmission (the email and all attachments) is intended solely for the addressee(s) and is both confidential and privileged. It is strictly forbidden to share any part of this message with any third party, without a written consent of the sender. If you are not the intended addressee, or if this transmission has been addressed to you in error, you must not disclose, reproduce, or use the transmission or read any attachment. Delivery of this transmission to any person other than the intended recipient(s) does not waive privilege or confidentiality. If you have received this transmission in error, please reply by e-mail and delete it.

[Quoted text hidden]

EXHIBIT D

OfficialBlog

PLATFORM NEWS, TOKEN RELEASES AND TRADING TIPS

OFFICIAL ANNOUNCEMENTS

System Updates – Lot Size Changes

© January 23, 2019

Dear Traders,

This week we will be performing another series of upgrades in order to provide improved lot sizing to our users.

The changes being made have a broad impact, affecting roughly 50 pairs and will require a brief period of downtime for all pairs while we restart our matching engine.

The release will occur in two steps:

1. We will restart the HitBTC matching engine, during which time users will see 2-3 minutes of trading downtime on the platform and API requests may time out.
2. Updates (documented below) will be made to a large number of instruments. This will require approximately 5 minutes of downtime for each of the listed pairs while these updates occur. You will not be able to place or cancel orders on these pairs during this short maintenance period. API users may also receive a "Symbol not found" response on these pairs during this time.

As with previous updates to instruments lot sizing:

- In order to guarantee correct execution behaviour for the orders during and after the update, we will be canceling the current orders and booking a replacement via an atomic transaction.
- All order parameters will be preserved through the update and users will not see any behavioural differences in order execution or future updates to these orders.
- Users will be notified of this cancel/replace transaction through an Execution Report for each order. The cancellation of the original order and the replacement will also be visible to users querying their order history via API or via the Cancelled and Filled Orders widget.

If you have any questions or queries, please reach out to our support team at support@hitbtc.com

For your convenience, we will inform you of the exact pairs and markets 3 hours and 15 min before the procedure via Twitter and Web notifications.

Expected works schedule:
24 January, between 12.00 UTC and 15.00 UTC

Symbol	Old step	New step	Old lot	New lot
ADA/BTC	0.00000001	0.000000001	100	1
ADA/ETH	0.00000001	0.000000001	100	1
ADA/USD	0.00000001	0.000000001	100	1
BCHABC/BTC	0.0001	0.000001	0.01	0.0001
BCHABC/USD	0.01	0.001	0.01	0.0001
BCHSW/BTC	0.00001	0.000001	0.01	0.001
BCHSW/USD	0.001	0.0001	0.1	0.001
BTC/USD	0.01	0.01	0.01	0.00001
DASH/ETH	0.000001	0.000001	0.01	0.001
EOS/ETH	0.000001	0.0000001	0.01	0.01
ETC/ETH	0.000001	0.0000001	0.01	0.01
ETH/BTC	0.000001	0.000001	0.001	0.0001
ETH/USD	0.01	0.001	0.001	0.0001
ETH/DAI	0.01	0.001	0.0001	0.0001
IDTA/BTC	0.00000001	0.000000001	10	0.1
IDTA/ETH	0.00000001	0.000000001	10	0.1
IDTA/USD	0.00000001	0.000000001	10	0.1
NEO/BTC	0.00001	0.0000001	0.1	0.01
NEO/ETH	0.0001	0.0000001	0.1	0.01
NEO/USD	0.01	0.00001	0.01	0.01
NEO/EOS	0.0001	0.00001	0.1	0.01
DMG/BTC	0.00000001	0.000000001	1	0.01
DMG/ETH	0.00000001	0.000000001	1	0.01
DMG/USD	0.00000001	0.000000001	1	0.01
QTUM/BTC	0.00000001	0.000000001	1	0.01
QTUM/ETH	0.00000001	0.000000001	1	0.01
QTUM/USD	0.00000001	0.000000001	1	0.01
STRAT/ETH	0.0001	0.0000001	0.1	0.01
TRX/BTC	0.00000001	0.000000001	1000	1
TRX/ETH	0.00000001	0.000000001	1000	1
TRX/USD	0.00001	0.0000001	100	1
TRX/EOS	0.00000001	0.000000001	100	1
XDN/BTC	0.0000000001	0.0000000001	100	10
XDN/ETH	0.00000001	0.000000001	100	10
XLM/BTC	0.00000001	0.000000001	100	0.1
XLM/USD	0.00000001	0.000000001	100	0.1
XLM/ETH	0.00000001	0.000000001	100	0.1
XMR/BTC	0.000001	0.000001	0.01	0.001
XMR/USD	0.01	0.0001	0.001	0.001
XMR/ETH	0.000001	0.000001	0.01	0.001
XMR/EOS	0.001	0.0001	0.01	0.001
XRP/BTC	0.00000001	0.000000001	1	0.1
XRP/ETH	0.00001	0.00000001	1	0.1
XRP/USD	0.0001	0.000001	1	0.1
XRP/DAI	0.0001	0.000001	1	0.1
XRP/EURS	0.0001	0.000001	1	0.1
XRP/EOS	0.00001	0.000001	1	0.1
XVG/BTC	0.00000001	0.000000001	1000	10
XVG/ETH	0.00000001	0.000000001	1000	10
XVG/USD	0.00000001	0.000000001	1000	10
ZEC/ETH	0.000001	0.000001	0.01	0.001
ZEC/EOS	0.001	0.0001	0.01	0.001
ZEC/DAI	0.001	0.0001	0.01	0.001
ZEC/EUR	0.001	0.0001	0.01	0.001
ZEC/USD	0.001	0.0001	0.01	0.001

PRICE TICKER

CATEGORIES

- [Official announcements](#)
- [Listings](#)
- [Trading Instruments](#)
- [How does it work?](#)

FOLLOW US

- [Twitter](#)
- [Facebook](#)
- [Telegram](#)
- [Reddit](#)
- [Github](#)