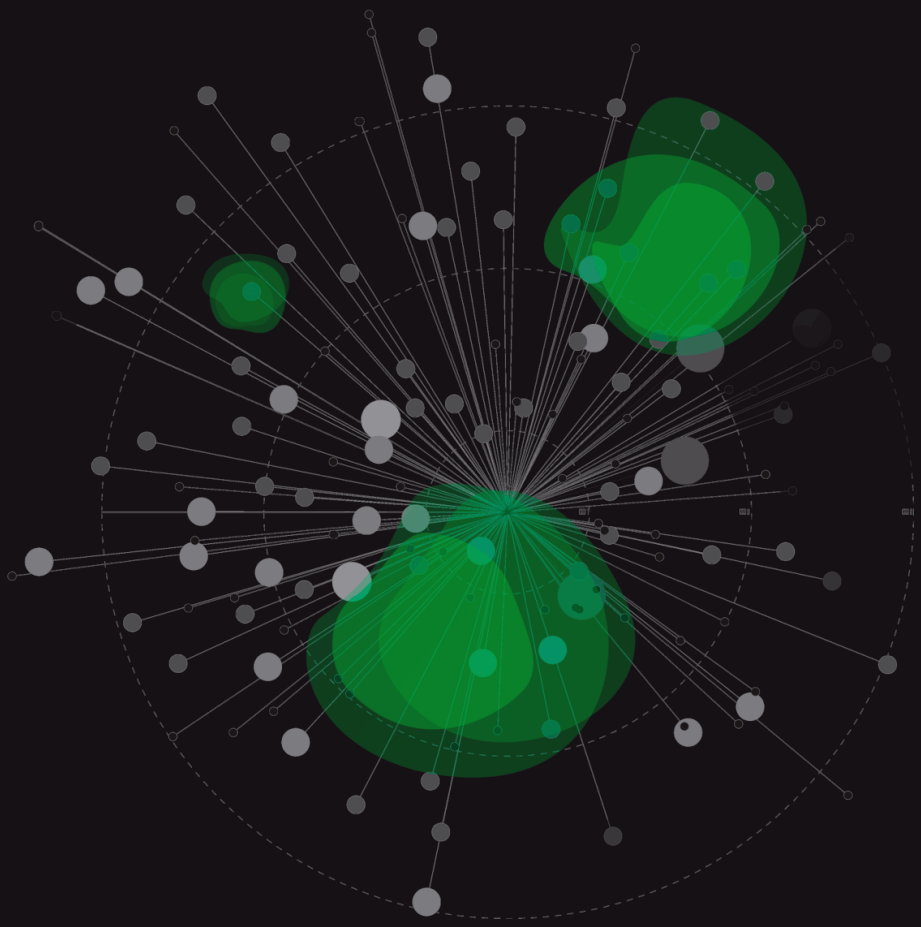
_more than just ratings

How to find an exchange's wallets



The CER system calculates exchange balance based on existing wallets in the system. All the wallets go through CER Evaluation System to prove their legitimacy. This evaluation corresponds to 4 level evaluation system. One of the ways to add the wallet into the CER Evaluation system is to add it using the CER Platform.

A Transparency Hacker can add wallets during his "Wallets Hunt." To make the reporting process easy and entertaining, you need to know the structure of wallets system, their main qualities, and attributes. The easiest way to describe the structure or reason for any system is to discover its history.

HISTORICAL BACKGROUND FOR HOT AND COLD WALLETS APPEARANCE

Looking back to September 2012, we find one of the largest hack attacks in cryptocurrency history, which happened to BitFloor and cost the company **24,000 BTC**. The hackers crashed the server of the exchange and later used the backup copy of the key to withdraw money from the BitFloor hot wallet. In 2015, Bitstamp became a victim of hackers who managed to steal **19,000 BTC** from the exchange's hot wallet by phishing. Another exchange, Coincheck suffered from an attack on the 27th of January 2018. As in most cases, the attack was aimed at the hot wallet and 523 million NEM tokens were successfully stolen by intruders. It is not complicated to find the weakest link in the chain of these events, right?

For this reason, the majority of the exchanges developed the cold storage system to protect the clients' funds and to minimize the risks during future hacks.

EXCHANGE WALLETS STRUCTURE

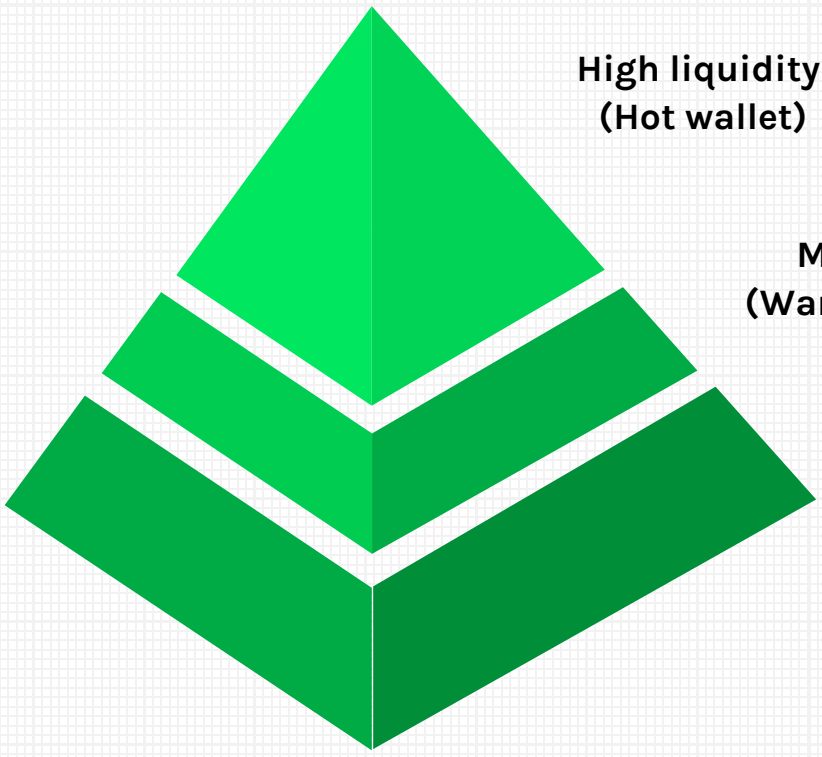
To start with, the definitions of wallet types can be considered very theoretical as a lot depends on the way you prefer to use this or that wallet. However, it is generally accepted to call the wallets which have access to the Internet — hot, and the ones which are not connected to the World Wide Web — cold. Furthermore, hot wallets are usually used for frequent and constant transactions (e.g. active trading), while the usage of cold ones implies long-term holdings with minimal interaction with the 3rd party sources. In this article, we will speak about the wallet types which are used by the exchanges, the attributes of each wallet type, and how to distinguish one wallet from another.

WHY IT'S IMPORTANT

Taking into account numerous successful attacks and the huge sums of money which were irretrievably lost, the question of exchange security must be treated as the first and highest priority.

Despite the fact that the majority of the exchanges claims that all the necessary protection steps have been implemented, at the moment there is no real opportunity to check whether the exchange is using a cold storage system or still prefers to keep clients' funds in hot wallets.

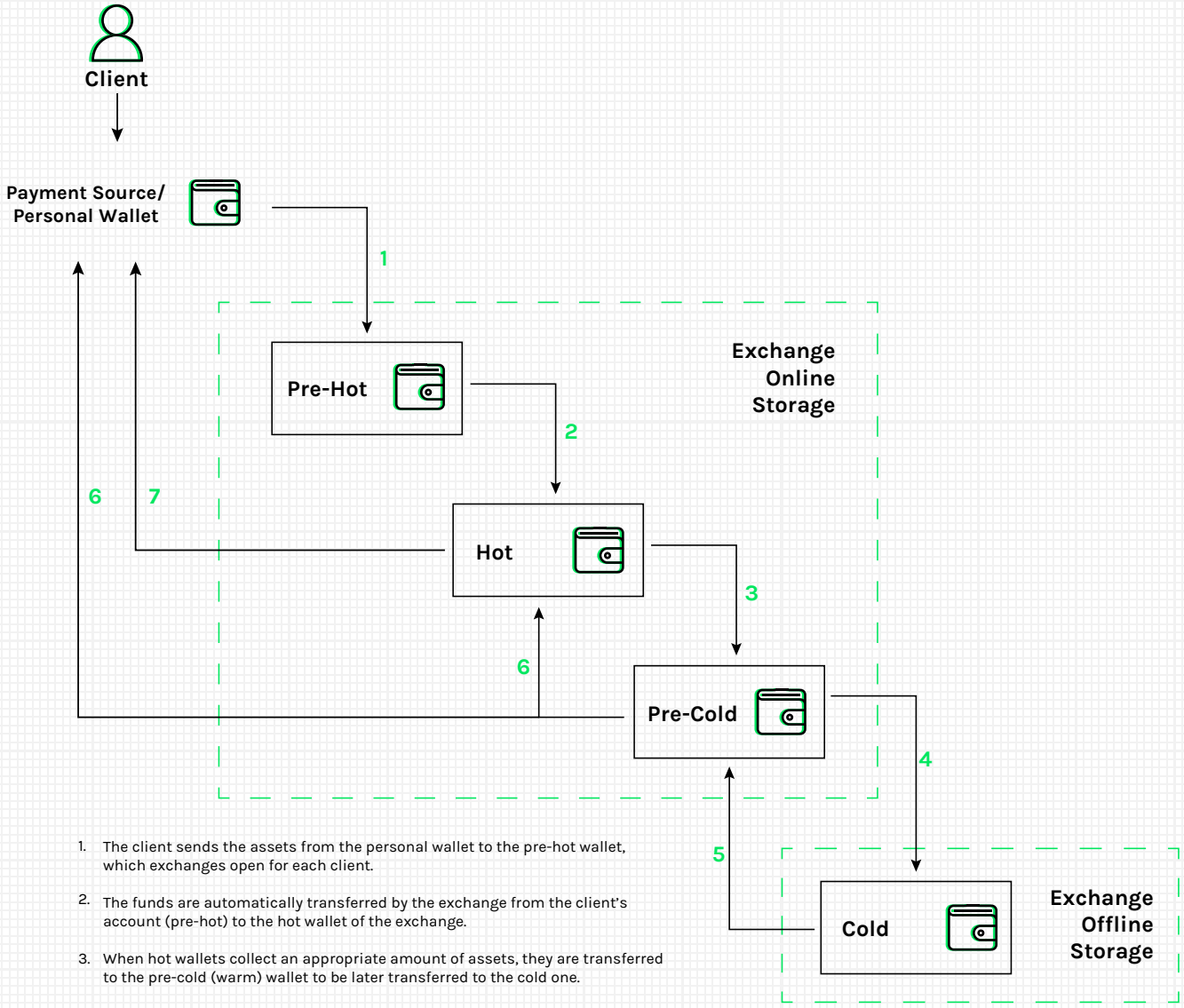
Another key thing to remember is that it is not possible to obtain precise data regarding exchange performance and sustainability (as this information can be easily discredited.) On obtaining the exchange's cold wallet addresses, we can find out the actual liquidity and volume indexes of the exchanges, which can be considered a revolution in the crypto industry.
Exchanges should apply another particular scheme to keep their assets that maintains a balance between safety and liquidity.



High liquidity (Hot wallet) includes the available online balance and the assets in the wallet/wallets accessible at any time. Warm wallets are used by the exchanges as transitions to Cold wallet. Cold wallet/wallets are the most safe and the most difficult to reach and hack. Thus, the main part of the exchange's assets is stored in the cold wallets and can be considered evidence of the exchange's liquidity and stability.

LET'S FIND THE WALLETS

To understand the full character of the wallets and their relations, let's move with the assets from the user's personal account to the exchange's cold wallet roundtrip.



1. The client sends the assets from the personal wallet to the pre-hot wallet, which exchanges open for each client.
2. The funds are automatically transferred by the exchange from the client's account (pre-hot) to the hot wallet of the exchange.
3. When hot wallets collect an appropriate amount of assets, they are transferred to the pre-cold (warm) wallet to be later transferred to the cold one.
4. The funds are transferred to the cold wallet of the exchange and are stored there.
5. The funds are transferred from the cold wallet to the pre-cold one when the exchange needs to reinforce quick liquidity or withdraw a bigger number of assets than liquidity on a hot wallet.
6. The funds are transferred from the pre-cold wallet to the hot one or to the user's personal payment source directly.
7. The funds are transferred from the hot wallet to the client's personal wallet.

WALLETS' ATTRIBUTES: HOW CAN WE DISTINGUISH ONE WALLET TYPE FROM ANOTHER?

"PRE-HOT" WALLETS (WHICH ARE GENERALLY THE CLIENT'S PERSONAL EXCHANGE ACCOUNT)

- Usually they are specifically generated by the exchange for each user and can be simply obtained.
- Sometimes they can be non-static, i.e. a new address is generated every time. As soon as the funds are transferred to the hot wallet, the address becomes invalid.
- They are used to top-up the balance and start trading.
- Only one-way transactions are implied (i.e. the client's funds are being sent from this account to other exchange hot wallets).

*As soon as the client top-ups his account balance, the exchange starts holding his funds in its system. Thus, in the case of a hack, the funds can be lost irrevocably.

EXCHANGE HOT WALLET

- The wallet to which the client's funds are sent directly. Consequently, we are able to track the connection between our personal exchange wallet and the exchange hot wallet.
- The wallet type which may directly interact with the client's personal payment source (the withdrawal transactions usually take place through the exchange hot wallets).
- Both inbound and outbound transactions are implied.

EXCHANGE "PRE-COLD" WALLET

- A transitive wallet between the hot and cold ones.
- Some of "pre-cold" wallets can send withdrawals directly to the client's payment method, however, usually, the withdrawals are sent using hot wallets.
- Both inbound and outbound transactions can be implied.

EXCHANGE COLD WALLET

- The wallet which is mostly used for cryptocurrency storage, thus, it should have a fewer number of inbound and outbound transactions than other wallet types.
- Cannot directly interact with the client's personal exchange account and the clients withdrawal payment method.
- Both inbound and outbound transactions are implied.

DISCLAIMER:

Please keep in mind that in order to obtain the reward for the accomplished work, the balance of the provided wallet addresses cannot be close to zero or have a small amount of money in storage. In the latter case, it is most likely that you have discovered the exchange pre-cold wallet, which is only the medium layer between hot and cold wallets and cannot be fully taken into consideration in calculating the exchange wallet balance.

HOW CAN WE FIND THE EXCHANGE COLD WALLET?

1. Firstly, we obtain our personal "account wallet" with the exchange.
2. We top-up our account balance with the exchange to start trading.
3. Along with the information from Points 1 and 2, we may figure out the address of the exchange hot wallet using the magic of blockchain system. The exchanges may have (and most likely they actually have!) several hot wallets.
4. Once we found the hot wallet of the exchange, we need to analyze whether there are additional hot wallets and, if yes, we must monitor the connections between them.
5. On finding several hot wallets, it is needed to find the connection with one or several pre-cold/cold wallets in the same way as in Points 3 and 4.

HOW TO REPORT AN EXCHANGE'S WALLET AND BECOME A TRANSPARENCY HACKER

We are happy to announce that currently, it is possible to report the exchange's hot and cold wallets on our website. It will allow you to become a Transparency Hacker, make your personal contribution to the crypto industry development and get a great reward! To become a part of our global transparency hacking initiative, we require creating an account on CER. You may check all the details along with the reward description by scrolling down our website (in the "Transparency Hackers" field).

WHAT COMES NEXT?

It isn't even worth noting how insecure and dangerous it is for the exchanges to keep the majority of clients' funds in hot wallets. In spite of this, some exchanges (even those which have already been hacked) still do not take the advantage of cold storage and continue to endanger their customers.

Understanding how the exchange wallet systems function and the ability to distinguish one type from another, will lead us to obtaining the cold wallet addresses of the exchanges.

Just imagine what would happen if we were able to see the unvarnished balance of each exchange wallet. Yet that is another story...

To be continued...

<The 2nd Part will be published soon. Please stay tuned!>

Join our global Transparency Hackers initiative now!

SIGN UP

BLOG_