The Blockchain Ledger

LINKING ASSETS INC.

A Jaisan Recovery Corp. April 09, 2021

LINKING ASSETS INC.
A Jaisan Recovery Corp.

In this Ledger

- Unhosted Wallets and Unclaimed Property
- Highlights: News & Developments

Linking Assets Inc. publishes *The Blockchain Ledger* with articles and information regarding blockchain, cryptocurrency, virtual currency, digital assets, etc. and their intersections with state unclaimed property laws. Keeping you informed of pertinent unclaimed property implications and related developments.

Unhosted Wallets and Unclaimed Property

By Christa DeOliveira, CIA, CCEP & Ari Mizrahi, CISSP, OSCP

States are including digital currencies in their statutes; although, there are technical challenges limiting a state's ability to transfer cryptocurrencies of unhosted wallets. Even though most blockchain ledgers are publicly visible, transparent, and globally distributed-no one, whether legally authorized to or not, can access the assets, stored value, or cryptocurrency held in a digital wallet without the private key. This presents a unique challenge in the context of unclaimed property laws.

A blockchain wallet is commonly defined as a digital wallet that allows users of the blockchain to store and manage their currency. Every blockchain has its own type of wallet and it is how users interact with the blockchain. With wallets, a user can send currency, receive currency, and perform other types of transactions on the blockchain. Within a digital wallet you can create an unlimited number of sub-accounts, for example, a savings account, a spending account, a vacation trip account, a retirement account.

To create these sub-accounts, a very long, complex character string is stored in two files and saved. One file, the private key, is a spending key. The private key allows the holder of the key to access the wallet/account to direct transacts on the value/cryptocurrency in that account. The other file/the public key, allows others to send currency from to your wallet and aids in receiving currency. This is the account number you give to someone to send you currency, like giving a business your bank account and routing number to receive regular old fiat currency.

The notion of a hosted wallet versus an unhosted is, specifically, who is holding those special files/keys. Many exchanges, like Coinbase and CashApp, offer cryptocurrency services. When your account is created, your digital wallet is generated, though your wallet keys are not revealed to you. Rather, these companies allow you to use their software and will send and receive currency on your behalf. They store your cryptocurrency for you much like a bank holds your fiat-banks don't give you keys to their vault, but they allow you to store it in their vault and perform transactions on your behalf.

Cryptocurrency, including Bitcoin, is financially inclusive and permissionless. Anyone is free to download a digital blockchain wallet software to create their own personal wallet on their computer or mobile device. Also, wallet hardware options are available. Some even store their keys on paper. These tools hold the keys to make an unhosted wallet. When you create an account using an unhosted wallet, you and only you have the special private key which allows you to send your currency. This is like keeping your fiat in your pocket or in a home safe.

Unhosted wallets block your cryptocurrency from being confiscated, frozen, or otherwise out of your control. (That is unless someone gains access to your private key.) While this type of wallet gives you exclusive control, the downside is that if you lose your private access key, then you have lost that money in your pocket and cannot get it back.

Both wallet types function in similar ways, but the ramifications of using one wallet type over another, is significantly different. Beyond unclaimed property, there are some benefits and risks to both wallet types.

Benefits of using hosted wallet
- User-friendly
- Convenient
- Exchange/financial institution manages the keys
- Financial institution has a degree of liability

Risks of using hosted wallet
- Hacks leading to thefts cannot be recovered (this risk can be mitigated by insurance)
- Cryptocurrency can be frozen or confiscated by authorized authorities or government
- Sending and receiving currency is limited to the terms of the exchange/financial institution and may be prevented at their discretion

Benefits of using unhosted wallet
- Pseudo-anonymity
- Complete control of your currency
- Assets cannot be frozen or confiscated
- Freedom to send and receive currency at will

Risks of using unhosted wallet
- You are liable in any mishandling or theft (these risks can be mitigated by insurance)
- You must manage your own private key

Currently, it is impossible to force any type of transfer, including escheat of unhosted wallets and it fundamentally violates the precepts of the blockchain structure. While it is possible to determine the most recent activity on an unhosted wallet, there is simply not a clear holder of record; rather, a distributed ledger across many different recordkeepers. In addition to data being housed on a distributed ledger, the private key is unknown for unhosted wallets and transfers can only be initiated by a the keyholder.

These factors will frustrate the process of any state attempting to escheat any unclaimed unhosted wallets.

Whereas, for cryptocurrency stored on an exchange/financial institution, there is a clear holder, and both the public and private keys are known to this holder-these assets could be escheated in accordance with unclaimed property statutes.

If you would like more information on blockchain, virtual currency, or unclaimed property, contact the authors, Christa DeOliveira, CIA, CCEP or Ari Mizrahi, CISSP, OSCP.

Highlights: News & Developments

With the proliferation of events and news in this sector, this section contains a few relevant highlights. We also include information on our NEWS page and LinkedIn.

SEC Commissioner Hester Pierce calls on Congress to streamline regulatory framework. "I think we're certainly falling behind the curve," said Hester Peirce. "We've seen other countries take a more productive approach to regulating crypto. Our approach has been to say no and tell people wait…we need to build a framework that is appropriate for this industry."[1] Currently, cryptocurrencies and financial services using blockchain technology are regulated by multiple federal and state agencies. Pierce would like to see Congress "draw some lines" and have "regulators come together and figure out what falls where."

The **IRS** continues to gain access to information on cryptocurrency exchanges to ensure tax obligations are met. The IRS seeks to identify "U.S. taxpayers who conducted at least the equivalent of $20,000 in transactions in cryptocurrency during the years 2016 to 2020." [2] After getting a court authorization to get the records from the cryptocurrency exchange Circle, the IRS is now pursuing access to Kraken data.[3]

[1] https://www.marketwatch.com/story/u-s-is-behind-the-curve-on-crypto-regulations-says-sec-commissioner-peirce-11617824160?mod=chris-matthews

[2] https://www.justice.gov/opa/pr/court-authorizes-service-john-doe-summons-seeking-identities-us-taxpayers-who-have-used-0

[3] https://www.fxstreet.com/amp/cryptocurrencies/news/irs-seeks-access-to-kraken-user-data-after-obtaining-circle-customer-records-202104050327