(U//LES) Crypto Cliff Notes – What Law Enforcement Needs to Know

(U//LES) Scope
The purpose of this bulletin is to provide necessary information for law enforcment officers to identify cryptocurrency and any related wallets, exchanges, and possible transactions.

(U//LES) Bottom Line Up Front (BLUF)
Cryptocurrency is being used in drug sales, human trafficking, fraud, darknet transactions, cybercrimes, terrorism and much more. Cryptocurrency is based on anonymity but is sometimes traceable. Investigating cryptocurrency in criminal activity will assist and add value to your investigations and prosecution.

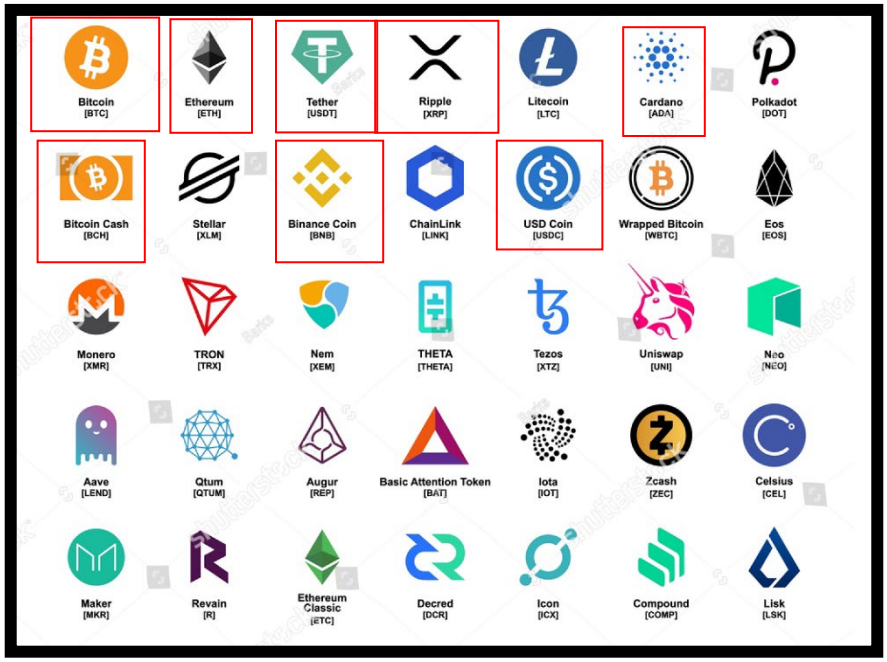
(U//FOUO) Definitions
Attribution: The process of labeling or assigning specific addresses to specific entities.[i]
Blockchain: A publicly available immutable ledger of completed transactions between two or more cryptocurrency addresses.[ii]
Cryptocurrency: A digital currency in which transactions are verified and records maintained by a decentralized system using cryptography, rather than by a centralized authority.[iii]
Cryptocurrency Wallets: An application on computers, mobile devices, or dedicated hardware that operates similarly to a digital wallet. Crypto wallets store the public and private keys needed to sign for cryptocurrency transactions and allow access to a user's cryptocurrency. Cryptocurrency is not physically stored in a wallet; it is bits of data scattered across a database. Cryptocurrency wallets gather the data associated with a user's account and displays their total amount on the application's interface. There are also different types of cryptocurrency wallets. [iv]
Mining: The process by which many, but not all, forms of cryptocurrency are created. This involves solving complex computational math problems. For each problem that is solved, more cryptocurrency value is added. This process takes immense computing power and electricity to conduct.[v]
Public Key: A cryptographic code that allows users to be able to receive cryptocurrency into their account.[vi] Also referred to as a "wallet address."
Private Key: A cryptographic code, known only to the user, that operates similarly to a password. This is the user's digital ID that allows them to authorize cryptocurrency transactions whether it be spending, withdrawing, or transferring funds. When a user initiates their first cryptocurrency transaction, a public and private key is created for them and is stored in a cryptocurrency wallet. These keys together are what ensure the security of a user's cryptocurrency.[vii]
Seed Phrase: A randomly generated list of 12-24 words that are associated to a user's wallet. This list of words can be used to recover or restore a cryptocurrency wallet if it is lost or damaged for any reason, as well as generate new private keys.[viii]
Token: A virtual currency asset, often associated with a virtual currency that runs on another virtual currency's blockchain.[ix]
Transaction Hash: Also known as a transaction ID, this is a unique, alphanumeric sequence associated with a transaction on a blockchain.[x]
Virtual Asset Service Provider (VASP): A platform used to buy, sell, trade, or exchange virtual currency.[xi]

(U//PAB) How Cryptocurrency Works

(U//PAB) For most forms of cryptocurrency to be created and add value, they must be mined. Individuals or groups will solve complex mathematical problems using computers to create the next transaction block on the block chain, and the owner of the block chain (Bitcoin, Ethereum, etc) will award the "miners" a variable denomination of crypto tokens or coins as compensation. Interested buyers can purchase cryptocurrency using "real" currency, and this value is maintained by the finite count of available coins and relative success or popularity of the cryptocurrency in use. Often, buyers will purchase cryptocurrency from a cryptocurrency exchange. To purchase cryptocurrency, they will first have to set up a wallet, which will most often be in either the form of software or hardware. To conduct the initial transaction, a public key will be assigned to them, as well as a private key. The public key will act as the address to which the other party involved shall send the purchased cryptocurrency. Once the buyer has received their cryptocurrency, it is then the private key they will use to authorize any further transactions. Once this, or any, cryptocurrency transaction has taken place it will be logged on the blockchain. For it to be approved, the majority of members of the blockchain network must confirm the transaction. Once this confirmation has been done the public block chains will display the transaction with a transaction hash, the public key (or wallet address) of all participants (senders and recipients), date and time, and denomination of cryptocurrency exchanged.[xii]

(U//LES) What to Look For

(U//LES) Types of Cryptocurrency:
Cryptocurrency has many different forms, with each worth a different value depending on the mining for that specific cryptocurrency. Additionally, the value of any particular coin is highly volatile, which may affect seizure paybacks. If you are searching a device, look for the icons to the right to be on the device. According to Forbes, in April 2023, the top ten cryptocurrencies are Bitcoin (BTC), Ethereum (ETH), Tether (USDT), Binance Coin (BNB), U.S. Dollar Coin (USDC), XRP (Ripple), Cardano (ADA), Dogecoin (DOGE), Polygon (MATIC), and Solana (SOL).[xiii]



(U//LES) Types of Cryptocurrency Wallets:
A wallet holds a private key, which is like a password or a signature to access cryptocurrencies.[xiv] There are different types of wallets, such as paper wallets, hardware wallets, and online wallets.

(U//LES) A paper wallet is when a person uses a physical medium to store a private key. This is likely the safest way to have a wallet, but not the most convenient, as cryptocurrency can only be used digitally.[xv] Analyst Note: Paper wallets could be notepads, stationary, slips of paper kept in a "real" wallet, paper files, or be physically taped to a device, etc. If you find a piece of paper with QR codes or hashes (example: 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969) you may have a paper wallet.

(U//LES) A hardware wallet is an external device, like a multifactor token (for example, an RSA token) that is supposed to be kept secured and only connected to a computer when cryptocurrency transactions are needed. [xvi] Examples of hardware wallets can be seen to the right. Analyst Note: Hardware wallets could be found on someone's person, in a bag/purse/briefcase/bookbag, in a vehicle, in a lock box, etc.

▲ Hardware Wallets ►

(U//LES) The last type of wallet is an online wallet; private keys are stored in an app or other software. Cryptocurrency can easily be sent or received into an online wallet.[xvii] Analyst Note: Online wallets can be found on devices, such as smartphones, computers, and tablets.

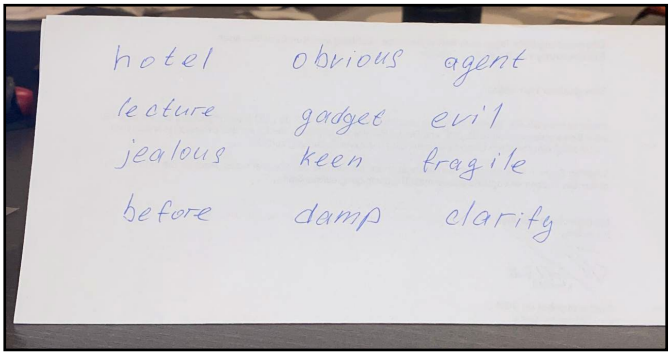
Cryptocurrency Wallet Apps to Look For

Ethereum	Blockchain.com	Coinbase Wallet
Coinbase	Bitcoin & Crypto DeFi Wa...	Crypto & Bitcoin Wallet A...
Binance	Trust	Crypto.com | DeFi Wallet
Bitcoin Wallet	ZenGo	Atomic Wallet
Luno - Bitcoin & Crypto ...	Exodus	BitPay - Bitcoin Wallet & ...
Paxful | Bitcoin Wallet	FreeWallet	Coinomi
MEW crypto wallet	Edge - Bitcoin & Crypto ...	Guarda Crypto Bitcoin W...
Coin Wallet	Uphold	Copay Bitcoin Wallet
Coinbase Pro	Ledger Live	CoinSmart - Buy Bitcoin ...
TokenPocket Wallet Cryp...	Lumi Crypto Bitcoin Wallet	Keplr Wallet
CoinPayments - Crypto ...	Matrixport	Bit2Me
Ember Fund - Invest in C...	WhiteBIT – buy & sell bitc...	7b
Bittrex Global	OKX	USDX Wallet - blockchain...
Cake Wallet	Mycelium Bitcoin Wallet	Crypto Tracker - Coin Sta...
MetaMask - Blockchain ...	Wirex Wallet	Crypto Pro
Bitcoin Wallet — Crypto ...	Dogecoin Wallet	Testnet Wallet
Airbitz - Bitcoin Wallet	HyperPay	Blockchain.com Exchange

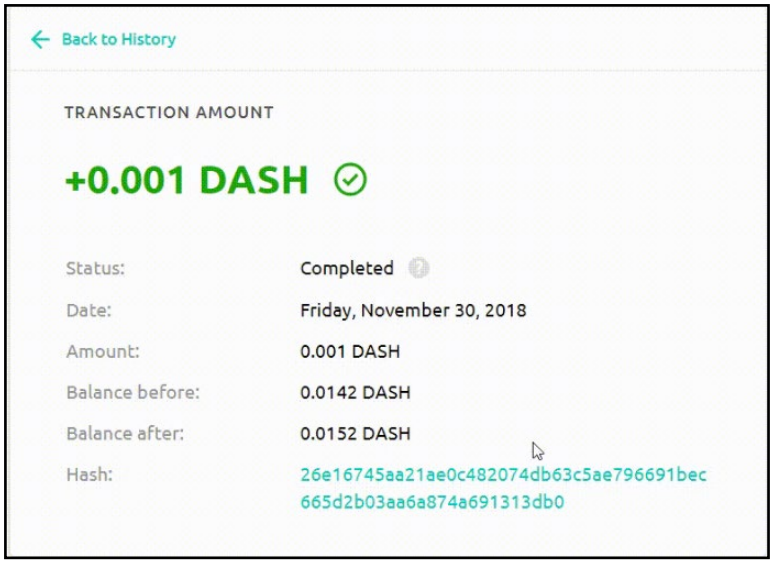
(U//LES) What is a Seed Phrase:

A seed phrase is used to recover broken or lost wallets; it is used as a security measure. A seed phrase contains 12 to 24 random words and may also be known as a mnemonic phrase when the combination of words is not random and resembles a sentence or short poem. It is common for seed phrases to be found on paper like the example shown here. [xviii]

Analyst Note: Seed phrases can be written on a piece of paper or in a Notes app on a device. If a seed phrase is found, keep looking for wallets (see above), cryptocurrency or wallet apps, and transaction receipts.



(U//LES) What is a Transaction Hash:
Transaction Hash is a unique identifier, similar to a receipt, that serves as proof a transaction was validated and added to the blockchain. In many cases, a transaction hash is needed in order to follow the movement of funds. A transaction hash can be used to provide confirmation the transaction was made (similar to receiving a receipt of purchase when you buy something at a store), look up transaction details, such as sending address, receiving address, amount, date and time, network fees, and confirmations. Transaction hash details can be viewed using a block explorer, which is a website where you can search the hash and see the ledger.[xix] Analyst Note: Transaction hashes may be found as a paper receipt, on a device as a screen shot, or in a wallet app.



(U//LES) Cryptocurrency ATMs

(U//LES) Bitcoin ATMs, cryptocurrency ATMs, and crypto kiosks, are used to exchange U.S. Dollars for cryptocurrency. In 2022, there were 50,000 of these machines in the U.S.[xx] In Missouri, we have 530 cryptocurrency ATMs, as of April 2023. To find where they are and how many you have in your area of responsibility (AOR) reference https://coinatmradar.com/country/226/bitcoin-atm-united-states/.[xxi]

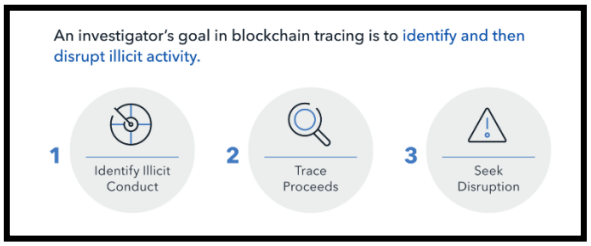
(U//LES) To use a cryptocurrency ATM, cash is inserted into the ATM, then a wallet address needs to be entered or if the wallet is on a phone, a QR code will appear on the ATM and can be scanned by the phone for the cryptocurrency to be added to the wallet. Some ATMs will allow purchase and selling of cryptocurrency, others are one-directional. A cryptocurrency ATM can also be used to send cryptocurrency to other people. The fees to use a cryptocurrency ATM may be up to 20% of the transaction value and typically are far greater than point-to-point transactions. [xxii]

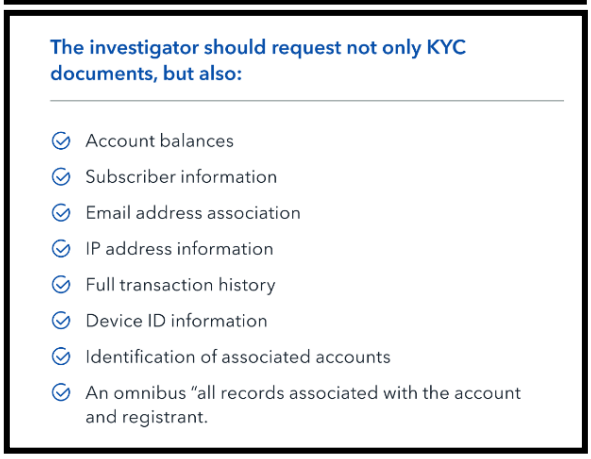
(U//LES) What to Do When You Find Cryptocurrency Related to Suspected Criminal Activity

(U//LES) If you find cryptocurrency on a device, a hardware wallet, a seed phrase, or any other cryptocurrency indicators, please contact the Missouri Information Analysis Center (MIAC), United States Secret Service (USSS) field office or Federal Bureau of Investigation (FBI) field office for assistance if needed.

(U//LES) When inquiring for data related a wallet, typically, a memo on official letterhead will suffice. However, a subpoena, court order, or search warrant will also be useful. Always ask for their Know Your Customer (KYC) Data, as well as account balances, subscriber information, email addresses, IP addresses, full transaction history, device ID, and ID of associated accounts in your official request.

(U//LES) To seize cryptocurrency law enforcment must execute a seizure warrant to the financial institution or exchange/wallet. The warrant should also contain a "non-disclosure" provision that forbids the bank from disclosing the existence of the warrant, which prevents any transfer or withdrawal of funds while the bank is still in the process of reviewing and complying with the warrant.





(U//LES) It is critically important to have a cryptocurrency wallet under control of the law enforcement authority ready to receive seized cryptocurrency assets before executing cryptocurrency seizure. Furthermore, the worth of the seized assets may exceed the value of asset typically secured by the department's evidence handling procedures. Note that anyone with access to a seized wallet's seed words, QR code, or public/ private key pair, may transact with that wallet's cryptocurrency resources. Therefore, robust chain of custody protection is critical when seizing cryptocurrency assets.

(U//LES) The seizure does not extinguish the account holder's interest in the property, only who has custody and control over it. Legally, the seized funds are controlled by the court that issued the warrant, though law enforcement will be responsible for safekeeping of the cryptocurrency assets and will usually transfer the funds into an account under control of the law enforcement agency, depending on the language of the warrant.

For additional information on legal process and seizures, please reference: https://www.cryptotrack.us/le-guides.

(U//FOUO) Resources

- https://www.cryptotrack.us/le-guides
- https://coinatmradar.com/country/226/bitcoin-atm-united-states/

If you need assistance with a cryptocurrency case or if you have any questions, please contact the MIAC OHS Cybersecurity Team at 573-526-0153 or securityintel@mshp.dps.mo.gov.

You can also request assistance through the MIAC Kaseware portal: https://app.kaseware.us/public/#miac/57a456c0-2908-4a6b-88ad-e33e866bfe6d.

(U//FOUO) This MIAC product pertains to Department of Homeland Security Standing Information Need(s): HSEC-01 and Missouri Standing Information Need(s): MIAC-SIN-01.

---

[i] TRM Labs Blockchain Investigators Flip Book
[ii] Ibid.
[iii] Dictionary.com
[iv] Vermont Intelligence Center Security Guide to Cryptocurrency, August 2022
[v] Ibid.
[vi] Ibid.
[vii] Ibid.
[viii] Ibid.
[ix] TRM Labs Blockchain Investigators Flip Book
[x] Ibid.
[xi] Ibid.
[xii] Vermont Intelligence Center Security Guide to Cryptocurrency, August 2022
[xiii] https://www.forbes.com/advisor/investing/cryptocurrency/top-10-cryptocurrencies/
[xiv] https://www.coinbase.com/learn/crypto-basics/what-is-a-crypto-wallet
[xv] Ibid.
[xvi] Ibid.
[xvii] Ibid.
[xviii] https://www.nerdwallet.com/article/investing/seed-phrase#:~:text=Here%20is%20an%20example%20of,could%20be%20in%20seed%20phrases
[xix] https://help.coinbase.com/en/coinbase/getting-started/crypto-education/what-is-a-transaction-hash-hash-id
[xx] https://www.bankrate.com/banking/what-are-bitcoin-atms/
[xxi] https://coinatmradar.com/country/226/bitcoin-atm-united-states/
[xxii] https://www.bankrate.com/banking/what-are-bitcoin-atms/#benefits-risks