Coinfirm

AML Risk Report generated by Coinfirm's AML/CTF Platform (https://www.coinfirm.com).
ID: *e8da2bcd2e889c34b2c2400b4224a090bc42a032b56a7012cd429ae59e071503*
Time: **2021-06-30T16:53:07.749Z** (UTC), Report Generation Block Height: **689228**.
Refer to Terms of Service for conditions of Report use.

AML Risk Enhanced Report for BTC address

1MEPCZZkXSf5n3FEZBb3WiyDzRv6ytxFWt

[redacted]

CURRENT BALANCE	0 BTC
USD VALUE	0 USD at 34386 USD/BTC rate

C-SCORE ANALYSIS

LIST OF IDENTIFIED RISKS

- Address belongs to obliged service with no KYC process
- Address with incoming transactions being multiple input-multiple output transactions
- Address with significant part of multiple input-multiple output incoming transaction
- Address with outgoing transactions being multiple input-multiple output transactions
- Address with significant part of multiple input-multiple output outgoing transaction
- Address belongs to over the counter exchange
- Address belongs to cryptocurrencies exchange
- Address with part of outgoing transactions in close proximity to addresses related to drugs trade
- Address with part of outgoing transactions in close proximity to addresses related to darknet markets
- Address with part of incoming transactions in close proximity to mixers or tumblers addresses
- Address with part of incoming transactions in close proximity to over the counter exchange addresses
- Address with part of outgoing transactions in close proximity to over the counter exchange addresses
- Address belongs to payment processor
- Address with part of outgoing transactions in close proximity to addresses found on deep web
- Address with dust funds tainted by incoming transactions from address directly related to drugs trade
- Address with dust funds tainted by incoming transactions from address directly related to darknet market
- Address with dust funds tainted by incoming transactions in close proximity to address participating in one or more CoinJoin transactions.
- Address with dust funds tainted by incoming transactions from address found on deep web

PROFILE ANALYSIS

[redacted] HTT[redacted]

OWNERSHIP INFORMATION

Name	[redacted]
Legal name	[redacted]ed
Industry risk	MEDIUM (Cryptocurrencies exchange)
Cluster	There are a total of 199 392 addresses belonging to same owner

OWNER PROFILES

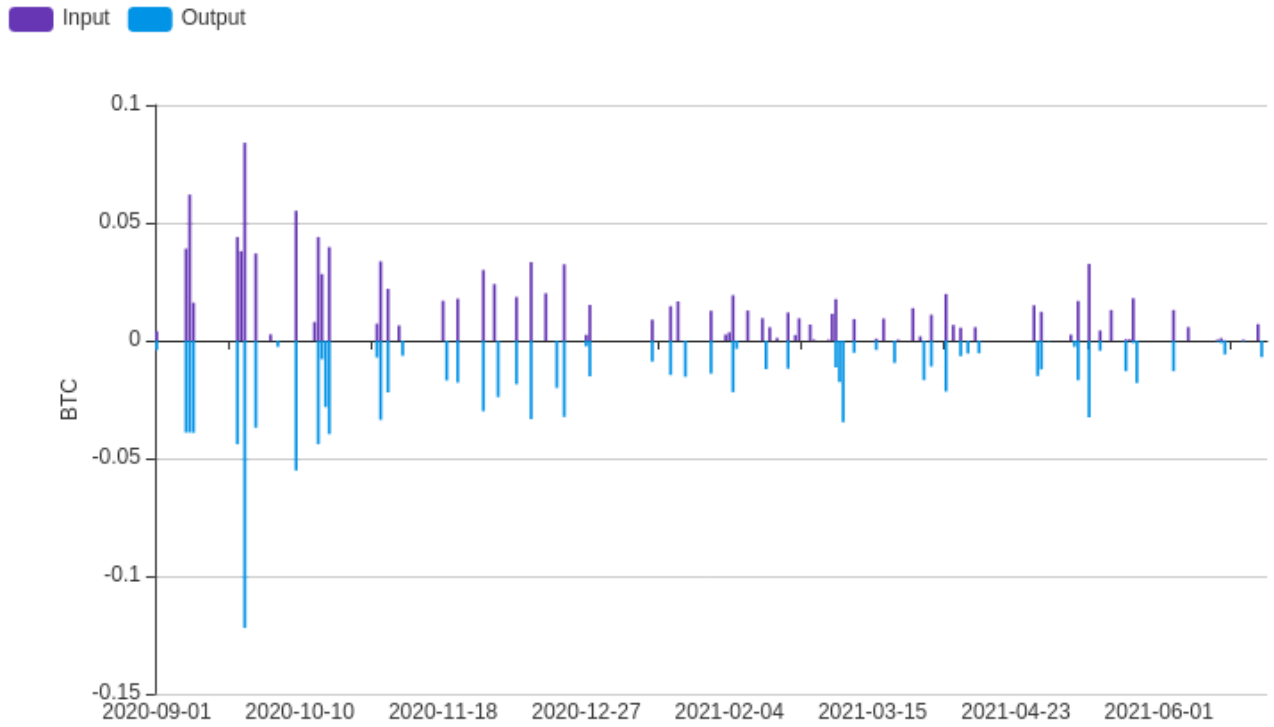
- Address owned by a company
- Cryptocurrencies exchange
- Over the counter exchange
- Receiving from mining pool
- Payment processor
- Online wallet

FINANCIAL ANALYSIS

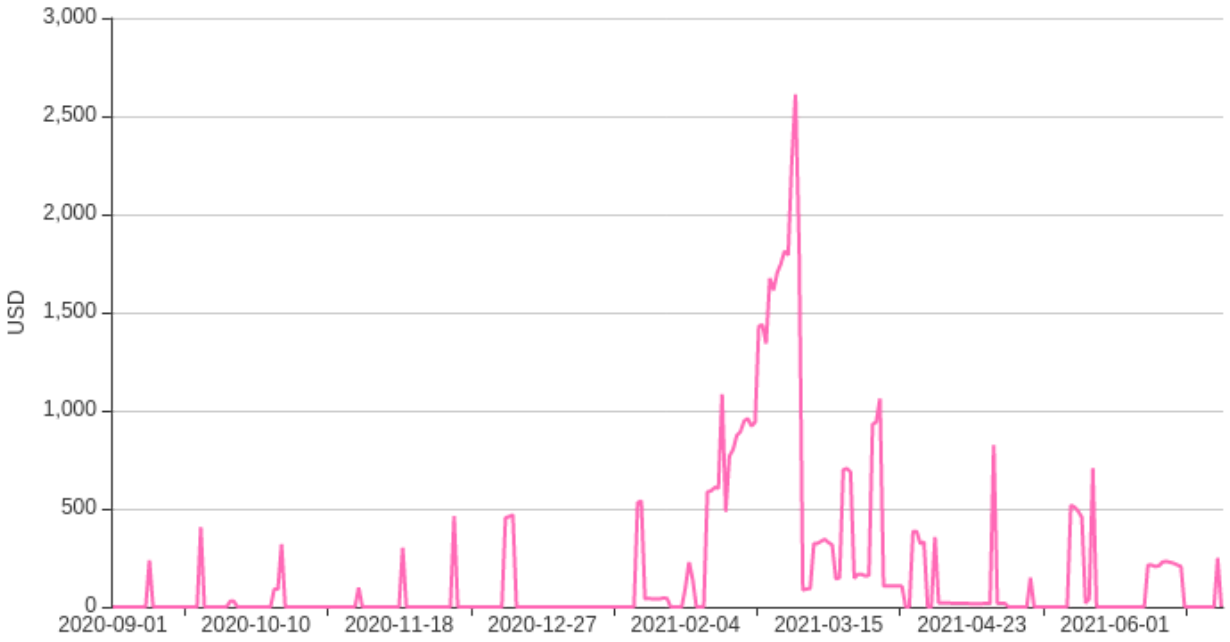
TOTAL TRANSACTIONS	174
TOTAL BTC TRANSFERS	174
BTC TURNOVER	2.354263 BTC $80 953.70

TOTAL BTC INPUT	1.177132 BTC $40 476.85	TOTAL BTC OUTPUT	1.177132 BTC $40 476.85
AVG BTC INPUT	0.01353 BTC $465.25	AVG BTC OUTPUT	0.01353 BTC $465.25
LARGEST	0.084 BTC $2 888.42	LARGEST	0.084 BTC $2 888.42
SMALLEST	0.000115 BTC $3.94	SMALLEST	0.000115 BTC $3.94
BTC INPUT TRANSFERS	87	BTC OUTPUT TRANSFERS	87

INPUT / OUTPUT



BTC BALANCE



 Informative

 Identified Risk

 Decreasing Factor

N/A Risk Verified But Not Identified

Money laundering

- N/A Industry risk - not a regulated activity
- N/A Charges and adverse media
- N/A High risk owner

No or limited KYC

- Address belongs to obliged service with no KYC process

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address is found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by an obliged service with no Know Your Client (KYC) process or account of its user;
  - The evaluated blockchain address is discovered through data analysis as being owned (through ownership of private keys corresponding to this address) an obliged service with no KYC process or account of its user;
  - An obliged entities such as digital currency exchanges, remittance companies, lending services or online cryptocurrencies wallets need to have a proper KYC process in place to meet regulatory requirements; lack of KYC process in obliged entities significantly increases the risk of using services of these entities for money laundering.

  Example: The evaluated blockchain address was found through data analytics to be a deposit address of the cryptocurrencies exchange which does not require providing identity documents to activate the user's account and enable user's to trade unlimited volumes.

- N/A Address with significant part of incoming transactions in close proximity to obliged service with no KYC process
- N/A Address with part of incoming transactions in close proximity to obliged service with no KYC process
- N/A Address with significant part of outgoing transactions in close proximity to obliged service with no KYC process
- N/A Address with part of outgoing transactions in close proximity to obliged service with no KYC process
- N/A Address belongs to obliged service with limited KYC process
- N/A Address with significant part of incoming transactions in close proximity to obliged service with limited KYC process
- N/A Address with part of incoming transactions in close proximity to obliged service with limited KYC process
- N/A Address with significant part of outgoing transactions in close proximity to obliged service with limited KYC process
- N/A Address with part of outgoing transactions in close proximity to obliged service with limited KYC process
- N/A Address belongs to obliged service which had no KYC and currently has limited KYC process
- N/A Address belongs to obliged service which had no KYC and has implemented full KYC process
- N/A Address belongs to obliged service which had limited KYC and has implemented full KYC process

Over the counter exchange

Address belongs to over the counter exchange

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address was found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by an over-the-counter exchange;
- The evaluated blockchain address was discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by an over-the-counter exchange;
- Over-the-counter is considered as direct trading of crypto and/or fiat between two parties which may occur outside of exchanges supervision (centralized and decentralized). It may combine access to unparalleled market liquidity with complete privacy;
- Over-the-counter exchanges may be considered as entities with increased AML risk as a result of the anonymity of their users.

N/A Address with significant part of incoming transactions in close proximity to over the counter exchange

Address with part of incoming transactions in close proximity to over the counter exchange addresses

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds the significant percentage of which originate from blockchain addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by an over the counter exchange or account of its user; or
- The evaluated blockchain address receives funds the significant percentage of which originate from blockchain addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by an over the counter exchange or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses owned by an over the counter exchange or account of its user;
- Over the counter exchanges are trading services allowing for direct trade between two parties, without the supervision of an exchange, frequently involving cash transactions;
- Over the counter exchanges are considered as entities with AML increased risk according to most of the related regulations; over the counter exchanges are considered as obliged institutions according to the AML FATF guidelines, EU directives and multiple other jurisdiction-specific regulations; over the counter exchanges are frequently used in money laundering as they act at the intersection of cryptocurrencies and traditional financial system and allow for greater anonymity than regular digital currency exchanges.

Example: The evaluated blockchain address received the equivalent of USD 50 k originating from the addresses which were found on deep web forum to be a deposit addressed of peer-to-peer cryptocurrencies exchange service advertising as an exchange providing outstanding anonymity of it's users; the pattern of transactions tree of the service was discovered through data analytics to be characteristic for large scale peer-to-peer exchange of cryptocurrencies; the amount constituted a significant portion of funds incoming to the evaluated address.

N/A Address with significant part of outgoing transactions in close proximity to over the counter exchange addresses

Address with part of outgoing transactions in close proximity to over the counter exchange addresses

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds the significant percentage of which reach to the

blockchain addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by an over the counter exchange or account of its user; or
- The evaluated blockchain address sends funds the significant percentage of which reach to the blockchain addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by an over the counter exchange or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses owned by an over the counter exchange or account of its user;
- Over the counter exchanges are trading services allowing for direct trade between two parties, without the supervision of an exchange, frequently involving cash transactions;
- Over the counter exchanges are considered as entities with AML increased risk according to most of the related regulations; over the counter exchanges are considered as obliged institutions according to the AML FATF guidelines, EU directives and multiple other jurisdiction-specific regulations; over the counter exchanges are frequently used in money laundering as they act at the intersection of cryptocurrencies and traditional financial system and allow for greater anonymity than regular digital currency exchanges.

Example: The evaluated blockchain address sent the equivalent of USD 50 k which credited the addresses which were found on deep web forum to be a deposit addressed of peer-to-peer cryptocurrencies exchange service advertising as an exchange providing outstanding anonymity of it's users; the pattern of transactions tree of the service was discovered through data analytics to be characteristic for large scale peer-to-peer exchange of cryptocurrencies; the amount constituted a significant portion of funds outgoing from the evaluated address.

N/A Decentralized exchange

N/A DeFi service

N/A Increased risk entity

N/A Increased risk country

Industry risk - regulated activity

- Address belongs to cryptocurrencies exchange

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address is found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by a cryptocurrencies exchange or account of its user;
  - The evaluated blockchain address is discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by a cryptocurrencies exchange or account of its user;
  - Digital currency exchanges are businesses that allow customers to trade cryptocurrencies (for example bitcoin) for other assets, such as conventional fiat money, or different cryptocurrencies;
  - Digital currency exchanges are considered as obliged institutions according to the AML FATF guidelines, EU directives and multiple other jurisdiction-specific regulations as they frequently hold blockchain private keys on behalf of their users and act at the intersection of cryptocurrencies and traditional financial system what may facilitate money laundering.

- N/A Address belongs to lending service
- N/A Address belongs to remittance service
- Address belongs to payment processor

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address is found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by a payment processor or account of its users;
  - The evaluated blockchain address is discovered through data analysis as being owned (through ownership of private keys corresponding to this address) a payment processor or account of its user;
  - Payment processors are subjects (often a third party) appointed by a merchant to handle transactions from various channels such as cryptocurrencies payments, credit cards, debit cards.
  - Payment processors are considered as obliged institutions according to the AML FATF guidelines, EU directives and multiple other jurisdiction-specific regulations as they frequently hold blockchain private keys on behalf of their users and act at the intersection of cryptocurrencies and traditional financial system what may facilitate money laundering.

- N/A Address belongs to payment cards provider
- N/A Address belongs to gambling service
- N/A Address belongs to gaming service
- N/A Address belongs to a licensed owner
- N/A Address belongs to an ATM chain

Transactions impeding track of funds - multiple input - multiple output transactions

Address with incoming transactions being multiple input-multiple output transactions

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds in one or more transactions, being so called "multiple input-multiple output" transactions;
- Multiple input-multiple output transaction is a transaction where funds are transferred from the set of more than one blockchain addresses owned by author of the transaction (input) to more than one blockchain addresses (output) in a single transaction; the same addresses may occur both in inputs and outputs of such transaction;
- It is a common method supporting funds layering to distribute the funds by using multiple input-multiple output transactions

Address with significant part of multiple input-multiple output incoming transaction

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds in one or more transactions, being so called "multiple input-multiple output" transactions; the value of such transactions constitutes a significant percentage of total transactions value received by the evaluated address;
- Multiple input-multiple output transaction is a transaction where funds are transferred from the set of more than one blockchain addresses owned by author of the transaction (input) to more than one blockchain addresses (output) in a single transaction; the same addresses may occur both in inputs and outputs of such transaction;
- It is a common method supporting funds layering to distribute the funds by using multiple input-multiple output transactions

Address with outgoing transactions being multiple input-multiple output transactions

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds in one or more transactions, being so called "multiple input-multiple output" transactions;
- Multiple input-multiple output transaction is a transaction where funds are transferred from the set of more than one blockchain addresses owned by author of the transaction (input) to more than one blockchain addresses (output) in a single transaction; the same addresses may occur both in inputs and outputs of such transaction;
- It is a common method supporting funds layering to distribute the funds by using multiple input-multiple output transactions

Address with significant part of multiple input-multiple output outgoing transaction

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds in one or more transactions, being so called "multiple input-multiple output" transactions; the value of such transactions constitutes a significant percentage of total transactions value sent from the evaluated address;
- Multiple input-multiple output transaction is a transaction where funds are transferred from the set of more than one blockchain addresses owned by author of the transaction (input) to more than one blockchain addresses (output) in a single transaction; the same addresses may occur both in inputs and outputs of such transaction;
- It is a common method supporting funds layering to distribute the funds by using multiple input-multiple output transactions

- N/A Transactions impeding track of funds - new addresses transactions
- N/A Transactions impeding track of funds - single incoming-outgoing transactions
- N/A Transactions impeding track of funds - rapid movement of funds
- N/A Transactions impeding track of funds - structuring payments
- N/A Transactions impeding track of funds - passing funds through miners
- N/A Transactions impeding track of funds - transactions impossible or difficult to decrypt
- N/A Transactions with distinctive patterns - high value addresses
- N/A Transactions with distinctive patterns - accumulating funds
- N/A Transactions with distinctive patterns - dormant status
- N/A Transactions with distinctive patterns - activity intervals
- N/A Transactions with distinctive patterns - inconsistent transactions patterns
- N/A Transactions with distinctive patterns - significant transactions value
- N/A Transactions with distinctive patterns - significant transaction fees
- N/A Transactions with distinctive patterns - round amounts
- N/A Initial Coin Offerings issuers & beneficiaries
- N/A Initial Coin Offerings contributors
- N/A Restricted networks
- N/A Special addresses
- N/A Connected Parties
- N/A Staking

N/A Financing of terrorism and proliferation

Direct links to crime and fraud offences

Weapon trade or trafficking

N/A

Crime against person

N/A

Drugs trade

- N/A Address directly related to drugs trade
- N/A Address being a part of funds layering/mixing scheme related to drugs trade
- N/A Address with significant part of incoming transactions in close proximity to addresses related to drugs trade
- N/A Address with part of incoming transactions in close proximity to addresses related to drugs trade
- N/A Address with significant part of outgoing transactions in close proximity to addresses related to drugs trade
- ! Address with part of outgoing transactions in close proximity to addresses related to drugs trade

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends funds the significant percentage of which reach to the addresses found or reported together with evidence or credible indication of being involved in illegitimate drugs trade; or
- The evaluated blockchain address sends funds the significant percentage of which reach to the addresses discovered through data analysis as being used in illegitimate drugs trade;
- There may exist a chain of one or several transactions (proximity) between the evaluated blockchain address and the addresses used in illegitimate drugs trade;
- What constitutes illegitimate trade in drugs varies widely, depending on local and national laws; this risk indicator attempts to reflect the requirements of regulations created in accordance with guidelines of FATF.

Example: The evaluated blockchain address sent the equivalent of USD 50 k which credited the addresses which were found on deep web as a trader payment address on drugs trade darknet service; the amount constituted a significant portion of funds outgoing from the evaluated address.

Darknet markets

- N/A Address directly related to darknet market
- N/A Address being a part of funds layering/mixing scheme related to darknet markets
- N/A Address with significant part of incoming transactions in close proximity to addresses related to darknet markets
- N/A Address with part of incoming transactions in close proximity to addresses related to darknet markets
- N/A Address with significant part of outgoing transactions in close proximity to addresses related to darknet markets
- Address with part of outgoing transactions in close proximity to addresses related to darknet markets

This risk indicator increases the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address receives funds the significant percentage of which reach to the addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by darknet market or account of its user; or
- The evaluated blockchain address receives funds the significant percentage of which originate from the addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by darknet market or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated blockchain address and the addresses being owned (through ownership of private keys corresponding to this address) by darknet market or account of its user;
- A darknet market is a commercial website on the web that operates via darknets such as Tor or I2P. It functions primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products; the examples of darknet markets are Silk Road, Agora, AlphaBay, Dream market, Valhalla.

Example: The evaluated blockchain address sent the equivalent of USD 50 k which credited the addresses which were found in a data leak as user account address on a specific darknet market; the amount constituted a significant portion of funds incoming to the evaluated address.

N/A Ransom

N/A Blackmail

N/A Scams & investment frauds

N/A Ponzi schemes

N/A Pump and dump

N/A Identity theft

N/A intellectual property piracy

N/A Credit card skimming or cloning

N/A Tax evasion

Mixers & Tumblers

- N/A Address belongs to mixer or tumbler
- N/A Address with significant part of incoming transactions in close proximity to mixers or tumblers addresses
- ! Address with part of incoming transactions in close proximity to mixers or tumblers addresses

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address receives funds the significant percentage of which originate from blockchain addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by a blockchain transactions mixer or account of its user; or
  - The evaluated blockchain address receives funds the significant percentage of which originate from blockchain addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by a blockchain transactions mixer or account of its user;
  - There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses owned by a blockchain transactions mixer or account of its user;
  - A blockchain transactions mixers (also referred as tumblers) are anonymous services, that confuse the trails of blockchain transaction. In most cases the client's funds are divided into smaller parts. These parts are mixed at random with similar parts of other clients. As a result, the client receives the funds with very low taint ratio (low traceability to client initial blockchain addresses);
  - According to existing regulations (e.g. 4th AML Directive of UE) mixing services are illegal.

  Example: The evaluated blockchain address received the equivalent of USD 50 k originating from the addresses which were found to be a deposit address of an online mixing service offering anonymization of digital currency ownership by mixing funds inputted by multiple users of that service; the pattern of transactions tree of the service was discovered through data analytics to be similar to government suspended bitcoin mixing services; the amount constituted a significant portion of funds incoming to the evaluated address.

- N/A Address with part of outgoing transactions in close proximity to mixers or tumblers addresses
- N/A Address with significant part of outgoing transactions in close proximity to mixers or tumblers addresses
- N/A Address participating in Lightning Network
- N/A Address with significant part of incoming transactions in close proximity to address participating in a opening Lightning Network
- N/A Address with significant part of incoming transactions in close proximity to address participating in Lightning Network
- N/A Address with significant part of outgoing transactions in close proximity to address participating in Lightning Network
- N/A Address with significant part of outgoing transactions in close proximity to address participating in a opening Lightning Network
- N/A Address participating in a Coinjoin transaction.
- N/A Address with significant part of incoming transactions in close proximity to address participating in one or more CoinJoin transactions.
- N/A Address with part of incoming transactions in close proximity to address participating in one or more CoinJoin transactions.
- N/A Address with significant part of outgoing transactions in close proximity to address participating in one or more CoinJoin transactions.

- N/A Address with part of outgoing transactions in close proximity to address participating in one or more CoinJoin transactions.

! Deep web

- N/A Address found on deep web
- N/A Address with significant part of incoming transactions in close proximity to addresses found on deep web
- N/A Address with part of incoming transactions in close proximity to addresses found on deep web
- N/A Address with significant part of outgoing transactions in close proximity to addresses found on deep web
- ! Address with part of outgoing transactions in close proximity to addresses found on deep web

  This risk indicator increases the risk assessment of the evaluated blockchain address when:
  - The evaluated blockchain address sends significant funds on blockchain addresses found or reported together with evidence or credible indication of being used in deep web;
  - Deep web is a part of the World Wide Web whose contents are not indexed by standard search engines for any reason;
  - There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses related to deep web;
  - Encountering the evaluated blockchain address in close proximity to addresses used on deep web increases its risk evaluation, as blockchain addresses used for illicit activities appear on deep web more frequently then random blockchain addresses.

  Example: The evaluated blockchain address sent the equivalent of USD 50 k which credited the addresses which were found on deep web hacking forum as a the address of one of the most active forum users, however the exact purpose of the address was not indicated; the amount constituted a significant portion of funds outgoing from the evaluated address.

N/A Name of illicit activity

N/A Shutdown or inactive service

N/A Cybercrime risk - ransomware

N/A Cybercrime risk - hacking & misappropriation

N/A Sanctions

N/A Bribery and corruption

N/A AML reporting thresholds

i Dust funds taint

N/A Terrorism financing

N/A Weapon trade or trafficking

N/A Crime against person

Drugs trade

Address with dust funds tainted by incoming transactions from address directly related to drugs trade

This risk indicator does not increase the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from the addresses found or reported together with evidence or credible indication of being involved in illegitimate drugs trade; or
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from the addresses discovered through data analysis as being used in illegitimate drugs trade;
- There may exist a chain of one or several transactions (proximity) between the evaluated blockchain address and the addresses used in illegitimate drugs trade;
- What constitutes illegitimate trade in drugs varies widely, depending on local and national laws; this risk indicator attempts to reflect the requirements of regulations created in accordance with guidelines of FATF.

Example: The evaluated blockchain address received the equivalent of USD 50 k originating from the addresses which were found on deep web as a trader payment address on drugs trade darknet service; the amount constituted a significant portion of funds incoming to the evaluated address.

Darknet markets

Address with dust funds tainted by incoming transactions from address directly related to darknet market

This risk indicator does not increase the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from the addresses found or reported together with evidence or credible indication of being owned (through ownership of private keys corresponding to this address) by darknet market or account of its user; or
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from the addresses discovered through data analysis as being owned (through ownership of private keys corresponding to this address) by darknet market or account of its user;
- There may exist a chain of one or several transactions (proximity) between the evaluated blockchain address and the addresses being owned (through ownership of private keys corresponding to this address) by darknet market or account of its user;
- A darknet market is a commercial website on the web that operates via darknets such as Tor or I2P. It functions primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed pharmaceuticals, steroids, and other illicit goods as well as the sale of legal products; the examples of darknet markets are Silk Road, Agora, AlphaBay, Dream market, Valhalla.

Example: The evaluated blockchain address sent the equivalent of USD 50 k originating from the addresses which were found in a data leak as user account address on a specific darknet market; the amount constituted a significant portion of funds incoming to the evaluated address.

N/A Ransom

N/A Blackmail

N/A Scams & investment frauds

N/A Ponzi schemes

N/A Pump and dump

N/A Identity theft

N/A Intellectual property piracy

N/A Credit card skimming or cloning

N/A Tax evasion

Mixers & Tumblers

N/A Address with dust funds tainted by incoming transactions from address belongs to mixer or tumbler

Address with dust funds tainted by incoming transactions in close proximity to address participating in one or more CoinJoin transactions.

This risk indicator does not increase the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from address that is discovered through data analysis as being significantly used as an input of CoinJoin transactions (being a member of a cluster where one or more addresses participated as inputs in CoinJoin transaction);
- CoinJoin is a trustless funds mixing method for combining multiple payments from multiple spenders into a single transaction to make it more difficult for outside parties to determine which spender paid which recipient or recipients;
- A blockchain transactions mixers (also referred as tumblers) are services or methods, that confuse the trails of blockchain transaction. In most cases the client\'s funds are divided into smaller parts. These parts are mixed at random with similar parts of other clients. As a result, the client receives the funds with very low taint ratio (low traceability to client initial blockchain addresses);
- According to existing regulations (e.g. 4th AML Directive of UE) mixing services are illegal.

Example: The evaluated blockchain address was found to receive the equivalent of USD 100k a payment address of an online mixing service offering anonymization of digital currency ownership by mixing funds inputted by multiple users of that service; the pattern of transactions tree of the service was discovered through data analytics to be match the characteristics of CoinJoin funds missing method.

N/A Address with dust funds tainted by incoming transactions in close proximity to address participating in a opening Lightning Network

Deep web

Address with dust funds tainted by incoming transactions from address found on deep web

This risk indicator does not increase the risk assessment of the evaluated blockchain address when:
- The evaluated blockchain address sends/receives dust funds (the amount of funds which is believed to be statistically immaterial for the risk evaluation) which reach to/originates from blockchain addresses found or reported together with evidence or credible indication of being used in deep web;
- Deep web is a part of the World Wide Web whose contents are not indexed by standard search engines for any reason;
- There may exist a chain of one or several transactions (proximity) between the evaluated address and the addresses related to deep web;
- Encountering the evaluated blockchain address in close proximity to addresses used on deep web increases its risk evaluation, as blockchain addresses used for illicit activities appear on deep web more frequently then random blockchain addresses.

Example: The evaluated blockchain address received the equivalent of USD 50 k originating from the addresses which were found on deep web hacking forum as a the address of one of the most active forum users, however the exact purpose of the address was not indicated; the amount constituted a significant portion of funds incoming to the evaluated address.

- N/A Cybercrime risk - ransomware
- N/A Cybercrime risk - hacking & misappropriation
- N/A High risk exchanges
- N/A No or limited KYC
- N/A Sanctioned country subject
- N/A Sanctioned subject
- N/A Politically exposed person (PEP)

N/A Blacklists and Whitelists

N/A Risk decreasing factors

APPENDIX 2

LAST 3 MONTHS

TOTAL TRANSACTIONS	51
TOTAL BTC TRANSFERS	51
TURNOVER	0.385761 BTC $13 264.78

TOTAL BTC INPUT	0.191977 BTC $6 601.31	TOTAL BTC OUTPUT	0.193784 BTC $6 663.47
AVG BTC INPUT	0.007679 BTC $264.05	AVG BTC OUTPUT	0.007453 BTC $256.29
LARGEST	0.032523 BTC $1 118.34	LARGEST	0.032523 BTC $1 118.34
SMALLEST	0.000115 BTC $3.94	SMALLEST	0.000115 BTC $3.94
BTC INPUT TRANSFERS	25	BTC OUTPUT TRANSFERS	26

LAST 6 MONTHS

TOTAL TRANSACTIONS	110
TOTAL BTC TRANSFERS	110
TURNOVER	0.79062 BTC $27 186.28

TOTAL BTC INPUT	0.39531 BTC $13 593.14	TOTAL BTC OUTPUT	0.39531 BTC $13 593.14
AVG BTC INPUT	0.007187 BTC $247.15	AVG BTC OUTPUT	0.007187 BTC $247.15
LARGEST	0.032523 BTC $1 118.34	LARGEST	0.032523 BTC $1 118.34
SMALLEST	0.000115 BTC $3.94	SMALLEST	0.000115 BTC $3.94
BTC INPUT TRANSFERS	55	BTC OUTPUT TRANSFERS	55

LAST 12 MONTHS

TOTAL TRANSACTIONS	174
TOTAL BTC TRANSFERS	174
TURNOVER	2.354263 BTC $80 953.70

TOTAL BTC INPUT	1.177132 BTC $40 476.85	TOTAL BTC OUTPUT	1.177132 BTC $40 476.85
AVG BTC INPUT	0.01353 BTC $465.25	AVG BTC OUTPUT	0.01353 BTC $465.25
LARGEST	0.084 BTC $2 888.42	LARGEST	0.084 BTC $2 888.42
SMALLEST	0.000115 BTC $3.94	SMALLEST	0.000115 BTC $3.94
BTC INPUT TRANSFERS	87	BTC OUTPUT TRANSFERS	87

FIRST INCOMING TRANSACTION

TRANSACTION HASH	49b46643132dc7486d4442ef3b606feb880c3d188495bbeaec35c69b846730f9
BLOCK TIME	01.09.2020 10:21:05
BLOCK HEIGHT	646263
TRANSACTION AMOUNT	0.004 BTC
TRANSACTION USD VALUE	$47.74

FIRST OUTGOING TRANSACTION

TRANSACTION HASH	7e248b358b18e9c4abd5f162eb1c08ac2c9096d8416a20201f169ba7e57605df
BLOCK TIME	01.09.2020 11:28:49
BLOCK HEIGHT	646271
TRANSACTION AMOUNT	0.004 BTC
TRANSACTION USD VALUE	$47.65

LAST INCOMING TRANSACTION

TRANSACTION HASH	f1d39444e6e8682a79bc2fc6f1441735224780700a505c4e9280aecefd24c0bf
BLOCK TIME	28.06.2021 10:55:11
BLOCK HEIGHT	689024
TRANSACTION AMOUNT	0.006982 BTC
TRANSACTION USD VALUE	$239.10

LAST OUTGOING TRANSACTION

TRANSACTION HASH	f8a61058492046d42b8f63bb01f10bf7b503852ff6c1316e8b894d952ae3b2d7
BLOCK TIME	29.06.2021 03:33:35
BLOCK HEIGHT	689100
TRANSACTION AMOUNT	0.006982 BTC
TRANSACTION USD VALUE	$241.80

LAST 24 HOURS ACTIVITY

INFLOW	0 BTC
OUTFLOW	0 BTC
AVERAGE INFLOW	0 BTC
AVERAGE OUTFLOW	0 BTC

DISCLAIMER

The Report is information only and is valid on the date of its issuance. Coinfirm does not give any express or implied warranty to the validity of any Report after the date of issuance of any Report.

Coinfirm takes all steps necessary to provide an independent analysis and information in the Report.

Coinfirm is not liable for any changes in assumptions and updates to this report in the case of new facts or circumstances occurring after the date of the Report or not known to Coinfirm at the time of generation of this Report.

Any decision taken by the recipient of this report is made solely on their own risk. The liability of Coinfirm is hereby excluded to the fullest extent permitted by the applicable law. The Report does not discharge any obligation of proper internal risk assessment and/or decision making process.

In no event will Coinfirm be liable to the recipients for:

- any act or alleged act, or any omission or alleged omission, that does not constitute wilful misconduct by Coinfirm, as determined in a final, non-appealable judgment by a court of competent jurisdiction,
- any indirect, special, punitive, incidental, exemplary, expectancy or consequential damages, including lost profits, lost revenues, loss of opportunity or business interruption, whether or not such damages are foreseeable, or
- any third-party claims (whether based in statute, contract, tort or otherwise).

This report should be read in full because any separate analysis of each of its parts can lead to erroneous conclusions.

Certain information, due to high risk (e.g. crime related), used for analysis, may not be able to be disclosed to the recipient.

To clarify any aspects contained in the Report please contact us at report@coinfirm.com.

GLOSSARY

Address	an address is like a bank account and for example a Bitcoin address starts with either a ‘1’ or a ‘3’ or a ‘bc1’ and is 26-35 alphanumeric characters in length. The address is generated from the private key, which is required to move assets assigned to this address to another address(es).
Anti-Money Laundering (AML)	the process of systems and controls that are applied to deter, disrupt and detect the flow of illicit value between collusive criminals that represents the proceeds of crimes and predicate offences such as tax evasion, sanctions evasion, theft, counterfeiting and fraud.
Blockchain	is a public ledger that records transactions that are performed. This is achieved without any trusted central authority as the maintenance of the blockchain is performed by a network of communicating nodes running the software. Network nodes validate transactions, add them to their copy of the ledger, and then broadcast these ledger additions to other nodes.
Combating the Financing of Terrorism (CFT)	the process of deterring and disrupting the financing of terrorism and proliferation. It is increasingly difficult to distinguish from money laundering activity due to the collusive conduct of terrorist financiers and transnational organized criminals, but it is typically distinguished from money laundering on the grounds that the sources of money laundering must be criminal, whereas the sources of finance for terrorism include donations from lawfully earning income. The goal of money laundering is typically a financial gain, while the goal of terrorism financing is typically ideological activity.
Customer Due Diligence (CDD)	a process to assess all of the risks associated with a client or relationship, including KYC, and that requires that the overall client conduct, and transactions are assessed to determine if this is unusual and reportable. CDD requires that obliged entities assess the risks before entering in to a relationship, and continuously thereafter in response to trigger events or suspicious activity for example. It is a continual process that is designed to assess and monitor changes in customer risks.
Decentralised Virtual Currencies	(cryptocurrencies) are distributed, open-source, mathematically-based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include: Bitcoin, Ethereum, Litecoin and Namecoin.
Distributed Ledger (Shared Ledger)	‘Ledgers’, or put simply, records of activity, were historically maintained on paper, more recently these were transferred to bytes on computers, and are now supported by algorithms in blockchains. They are essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the

	ledger are maintained cryptographically using ‘keys’ and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network. (Taken from UK Government: ‘Distributed Ledger Technology: beyond block chain’).
Electronic money (e-money)	is an electronic store of monetary value, based on technological mechanism for holding and accessing fiat currency.
Enhanced Customer Due Diligence (EDD)	a higher standard of due diligence, including identity verification and investigation that is required to be performed for those clients and relationships that have been identified as presenting the greatest risk of financial crimes. These risks include among others PEPs, Correspondent Banking, non-face-to-face activities such as virtual currency and private banking.
Exchanger / virtual currency exchange	is a website service, or an entity, engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wire payments, credit cards, and other virtual currencies. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts. Examples include: Bitstamp, GDAX, Kraken, OKCoin and ItBit.
Fiat Currency	is legal tender that is backed by the central government who issued it. Examples are the US Dollar, Japanese Yen and UK Sterling.
‘Fifth’ EU Money Laundering Directive (5MLD)	an amendment to the 4MLD that was agreed in response to the terrorist attacks across Europe in 2015 and 2016. The new law must be transposed by member states by 10th January 2020, and new measures include the requirement for virtual currency exchange services and virtual currency custodian wallet providers to be treated as ‘obliged entities’.
FinTech	refers to new applications, processes, products or business models that are being applied to improve the efficiency and security of financial services.
Fourth EU Money Laundering Directive (4MLD)	European response to the FATF 40 Recommendations from February 2012 and was required to be transposed by EU member states by 26th June 2017.
Hash	A hash value (or simply hash), also called a message digest, is a string of characters generated from a string of digital data, e.g. a pdf file. The hash is substantially smaller than the text itself and is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value and it is extremely difficult to reverse to identify the source message.

Know Your Customer (KYC)	the identification and verification of the natural person, legal entity or legal arrangement through identifying information, such as name and address, and the verification of these details to identify fraud, misrepresentation etc.
Money Laundering	a process to disguise the illicit source of value, either by self-laundering or through the placement, layering or integration process, conducted by criminals who ultimately wish to use this value for self-gratification, or to continue to finance their illicit activities.
Money Laundering Reporting Officer (MLRO)	the chief compliance officer responsible for all AML/CFT activities and responsible for ensuring that an obliged entity is not used by criminal or the financiers of terrorism.
Nodes	are computers in the blockchain network which receive new transactions and blocks, validate these transactions and blocks and spread valid transactions and blocks to connected nodes and ignore invalid transactions and blocks. It is generally considered that the more nodes exist in the network, the more secure the is the system.
Politically Exposed Person (PEP)	a person of high public office who may be able to influence the misappropriation of public funds whilst in office, or the awarding of public contracts. Include members of government, ruling classes such as Presidents, Royalty, Ministers of the Government and military and judiciary. The families of PEPs, and their close business associates, are also included due to the close affinity and trust that they may enjoy in their relationship, and which may lead to the PEP using these relationships as ‘front’ or ‘informal’ nominees.
Private Key	a private key is a cryptographic code that functions as a secret password that allows the user to sign a cryptocurrency transaction and transfer funds to another cryptocurrency address. Using the private key proves ownership of cryptocurrency.
Sanctions	when applied to financial services, represent a prohibition on providing regulated services to the subject of the sanction, and the requirement to freeze and report any assets that are held to the local jurisdiction sanctions administrator, such as OFAC or HMT.
Simplified Due Diligence (SDD)	a lower level of customer due diligence verification that can be performed where there is no, or a lesser, risk of money laundering.
Trading platforms	function as marketplaces, bringing together buyers and sellers of virtual currencies by providing them

	with a platform on which they can offer and bid among themselves. In contrast to exchanges, the trading platforms do not engage in the buying and selling themselves. Some trading platforms give their customers the option of locating potential customers nearby. Examples include LocalBitcoins.com and Mycelium Local Trader.
Transaction Fee	Is earned by miners when a transaction is completed. The minimum transaction fee required is determined by the "size" (kilobytes) of the transaction data. Most small transactions require a fee of about 0.0001 BTC and transactions with larger fees are given priority to be added to the block, so they are usually confirmed faster than transactions with low fees.