




AML Risk Report generated by Coinfirm's AML/CTF Platform (<https://www.coinfirm.com>).  
ID: `b4d23daf3d6dc54d19d2343cd0e00239902b7d808b6ad63b2021cf83c24b676d`  
Time: **2021-09-08T18:10:06.611Z** (UTC), Report Generation Block Height: **13186664**.  
Refer to Terms of Service for conditions of Report use.

## AML Risk Enhanced Report for ETH address

 **2708cace7b42302af26f1ab896111d87faeff92f**







 **Unidentified**

Address belongs to a hacker (DAO Maker Exploit 03.09.2021).

CURRENT BALANCE	0.953493 ETH
USD VALUE excl tokens	3 323.96 USD at 3486.09 USD/ETH rate
TOKENS	1 types
TOTAL INCL TOKENS	3 993 652.13 USD



LIST OF IDENTIFIED RISKS

-  Address being a part of funds layering/mixing scheme related to hacked or misappropriated address
-  Address belongs to hacker
-  Address with high value current balance
-  Address with at least one incoming transaction equal to or exceeding 10k USD
-  Address with significant part of single incoming transactions equal to or exceeding 10k USD
-  Address with dust funds tainted by incoming transactions from address belongs to mixer or tumbler



UNIDENTIFIED

---

**OWNERSHIP INFORMATION**

Name Unidentified

---

Legal name N/A

---

---

**ADDRESS PROFILES**

- Hacker
-

 FINANCIAL ANALYSIS

---

TOTAL TRANSACTIONS 30

---

TOTAL ETH TRANSFERS 30

---

ETH TURNOVER 1.958981 ETH  
\$6 829.18

---

 TOTAL ETH INPUT	1.948981 ETH \$6 794.32	 TOTAL ETH OUTPUT	0.01 ETH \$34.86
---	----------------------------	--	---------------------

---

AVG ETH INPUT	0.64966 ETH \$2 264.77	AVG ETH OUTPUT	0.000357 ETH \$1.25
---------------	---------------------------	----------------	------------------------

---

LARGEST	1.009431 ETH \$3 518.97	LARGEST	0.01 ETH \$34.86
---------	----------------------------	---------	---------------------

---

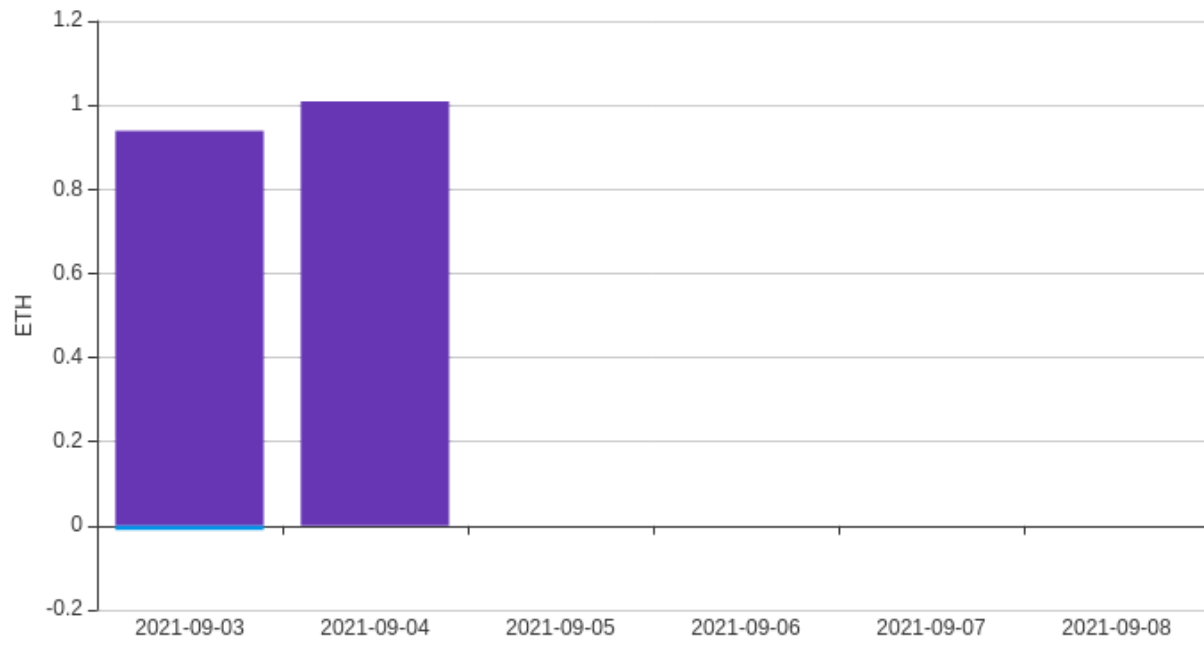
SMALLEST	0.0001 ETH \$0.35	SMALLEST	0 ETH \$0.00
----------	----------------------	----------	-----------------

---

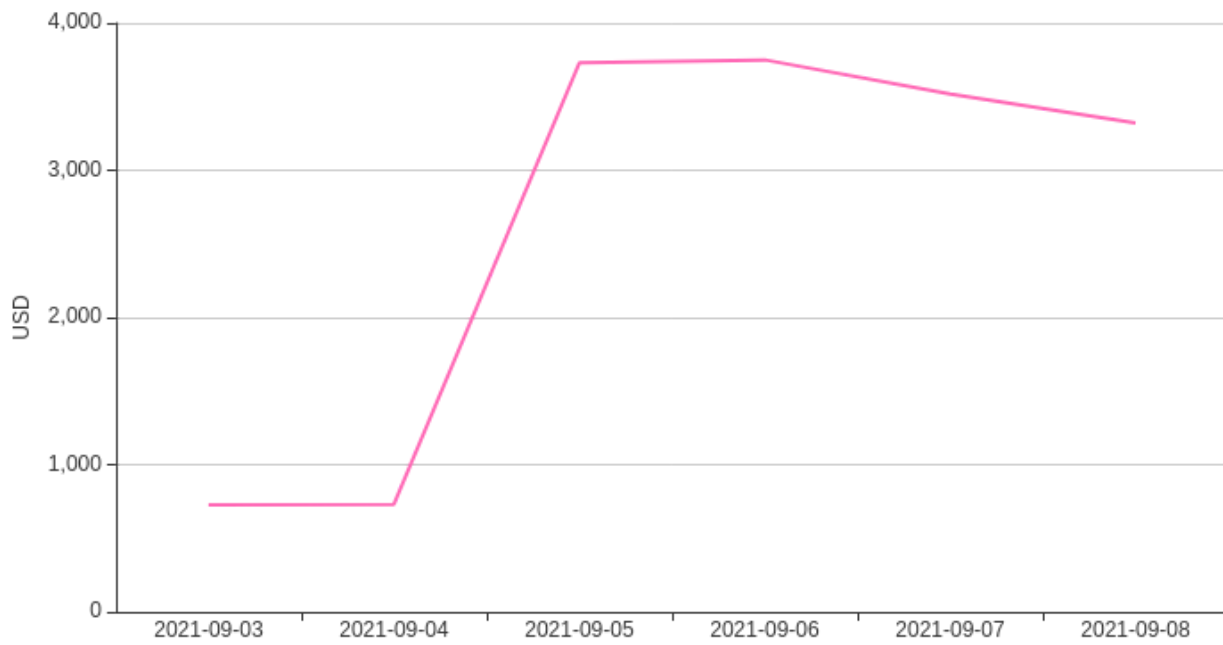
ETH INPUT TRANSFERS	3	ETH OUTPUT TRANSFERS	28
---------------------	---	----------------------	----

## INPUT / OUTPUT

Input Output



## ETH BALANCE

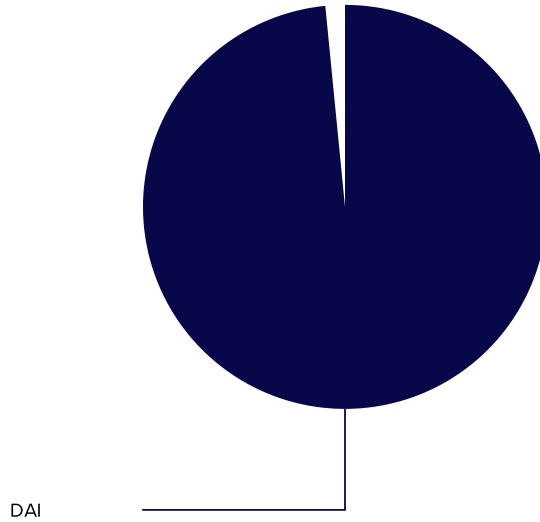




TOKENS THAT HAVE BEEN USED ON THIS ADDRESS.

SYMBOL	NAME	RATE (USD/TOKEN)	CURRENT BALANCE (IN TOKENS)	CURRENT VALUE (IN USD)
DAI	DaiStablecoin	1	3 990 328.171141	\$3 990 328.17

TOKENS AMOUNT





Informative



Identified  
Risk



















Decreasing  
Factor



Risk Verified But  
Not Identified

## Money laundering

-  Industry risk - not a regulated activity
-  Charges and adverse media
-  High risk owner
-  No or limited KYC
-  Over the counter exchange
-  Decentralized exchange
-  DeFi service
-  Increased risk entity
-  Increased risk country
-  Industry risk - regulated activity
-  Transactions impeding track of funds - multiple input - multiple output transactions
-  Transactions impeding track of funds - new addresses transactions
-  Transactions impeding track of funds - single incoming-outgoing transactions
-  Transactions impeding track of funds - rapid movement of funds
-  Transactions impeding track of funds - structuring payments
-  Transactions impeding track of funds - passing funds through miners

 Transactions impeding track of funds - transactions impossible or difficult to decrypt

 Transactions with distinctive patterns - high value addresses

 Address with high value current balance

This risk indicator increases the risk assessment of the evaluated blockchain address when:

- The evaluated blockchain address has currently the balance of funds equal to or exceeding 1 Mil USD
- It is relatively more frequent in a group of users involved in money laundering to achieve or maintain the high value balance of funds on the address, than it is in a group of random users.

 Address with high value historic balance

 Address maintaining high value balance for a long period of time

 Transactions with distinctive patterns - accumulating funds

 Transactions with distinctive patterns - dormant status

 Transactions with distinctive patterns - activity intervals

 Transactions with distinctive patterns - inconsistent transactions patterns

 Transactions with distinctive patterns - significant transactions value

 Transactions with distinctive patterns - significant transaction fees

 Transactions with distinctive patterns - round amounts

 Initial Coin Offerings issuers & beneficiaries

 Initial Coin Offerings contributors

 Restricted networks

 Special addresses

 Connected Parties

 Staking

 High risk exchanges

 Financing of terrorism and proliferation

 Direct links to crime and fraud offences



- N/A Weapon trade or trafficking
- N/A Crime against person
- N/A Drugs trade
- N/A Darknet markets
- 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
- N/A Mixers & Tumblers
- N/A Deep web
- N/A Name of illicit activity
- N/A Shutdown or inactive service
- N/A Cybercrime risk - ransomware

## ! Cybercrime risk - hacking & misappropriation

N/A Address which was hacked or misappropriated

! Address being a part of funds layering/mixing scheme related to hacked or misappropriated address

This risk indicator increases the risk assessment of the evaluated blockchain address when:

- The evaluated blockchain address was discovered through data analysis with evidence or credible indication that it was used for the purpose of layering funds originating from a hack, exploit, or being misappropriated.

- Layering involves distancing illegal proceeds from their source by creating complex levels of financial transactions designed to disguise the audit trail and to provide anonymity.

- Digital currency addresses of online services are frequently victims of hackings and misappropriation aimed to steal or misuse private keys required to sign and send blockchain transaction to the address managed by an illegitimate beneficiary.

N/A Address with significant part of incoming transactions in close proximity to addresses which were hacked or misappropriated

N/A Address with part of incoming transactions in close proximity to addresses which were hacked or misappropriated

N/A Address related to unauthorized withdrawal

N/A Address being a part of funds layering/mixing scheme related to unauthorized withdrawal

N/A Address with significant part of incoming transactions in close proximity to addresses related to unauthorized withdrawal

! Address belongs to hacker

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 used by a hacker;

- The evaluated blockchain address is discovered through data analysis as being used by a hacker;

- While the term "hacker" can refer to any computer programmer, for the purpose of this risk indicator it should be considered as someone involved in illicit activity related to unwanted breaking into computer systems. The term "hacker" may also refer to a person or group being responsible for the execution of an exploit attack targeted at DeFi platforms or smart contracts. Exploit attack consists of exploiting the vulnerabilities in the technical structure of a blockchain system using the existing functions of the protocol, very often including the flash loan feature.

N/A Address with significant part of incoming transactions in close proximity to hacker's addresses

N/A Address with part of incoming transactions in close proximity to hacker's addresses

N/A Address with significant part of outgoing transactions in close proximity to hacker's addresses

N/A Address with part of outgoing transactions in close proximity to hacker's addresses

N/A Sanctions

N/A Bribery and corruption

i AML reporting thresholds

N/A AML reporting thresholds (EUR)

## AML reporting thresholds (USD)

-  Address with at least one incoming transaction equal to or exceeding 10k USD

This risk indicator increases the risk assessment of the evaluated blockchain address when:

- The evaluated blockchain address receives funds in one or more single transactions, the value of each one equals to or exceeds 10k USD, at the exchange rate from the time of transaction;
- According to the existing regulations in certain jurisdictions such as United States, each transaction the value of which equals to or exceeds 10k USD, should be reported to the appropriate financial supervision authority.

-  Address with significant part of single incoming transactions equal to or exceeding 10k USD












This risk indicator increases the risk assessment of the evaluated blockchain address when:

- The evaluated blockchain address receives funds in one or more single transactions, the value of each one equals to or exceeds 10k USD, at the exchange rate from the time of transaction; the value of such transactions constitutes a significant percentage of total transactions value received by the evaluated address;
- According to the existing regulations in certain jurisdictions such as United States, each transaction the value of which equals to or exceeds 10k USD, should be reported to the appropriate financial supervision authority.

-  Address with at least one outgoing transactions equal to or exceeding 10k USD

-  Address with significant part of single outgoing transactions equal to or exceeding 10k USD

## Dust funds taint

-  Terrorism financing
-  Weapon trade or trafficking
-  Crime against person
-  Drugs trade
-  Darknet markets
-  Ransom
-  Blackmail
-  Scams & investment frauds
-  Ponzi schemes
-  Pump and dump
-  Identity theft

 Intellectual property piracy

 Credit card skimming or cloning

 Tax evasion

 Mixers & Tumblers

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

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 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 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 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.

 Deep web

 Cybercrime risk - ransomware

 Cybercrime risk - hacking & misappropriation

 High risk exchanges

 No or limited KYC

 Sanctioned country subject

 Sanctioned subject

N/A Politically exposed person (PEP)

N/A Blacklists and Whitelists

N/A Risk decreasing factors

---

LAST 3 MONTHS

TOTAL TRANSACTIONS 30



---

TOTAL ETH TRANSFERS 30

---

TURNOVER 1.958981 ETH  
\$6 829.19

---

 TOTAL ETH INPUT	1.948981 ETH \$6 794.32	 TOTAL ETH OUTPUT	0.01 ETH \$34.86
---	----------------------------	--	---------------------

---

AVG ETH INPUT	0.64966 ETH \$2 264.77	AVG ETH OUTPUT	0.000357 ETH \$1.25
---------------	---------------------------	----------------	------------------------

---

LARGEST	1.009431 ETH \$3 518.97	LARGEST	0.01 ETH \$34.86
---------	----------------------------	---------	---------------------

---

SMALLEST	0.0001 ETH \$0.35	SMALLEST	0 ETH \$0.00
----------	----------------------	----------	-----------------

---

ETH INPUT TRANSFERS	1	ETH OUTPUT TRANSFERS	29
---------------------	---	----------------------	----

---

LAST 6 MONTHS

TOTAL TRANSACTIONS 30

---

TOTAL ETH TRANSFERS 30

---

TURNOVER 1.958981 ETH  
\$6 829.19

⬇ TOTAL ETH INPUT 1.948981 ETH \$6 794.32 ⬆ TOTAL ETH OUTPUT 0.01 ETH \$34.86

---

AVG ETH INPUT 0.64966 ETH \$2 264.77 AVG ETH OUTPUT 0.000357 ETH \$1.25

---

LARGEST 1.009431 ETH \$3 518.97 LARGEST 0.01 ETH \$34.86

---

SMALLEST 0.0001 ETH \$0.35 SMALLEST 0 ETH \$0.00

---

ETH INPUT TRANSFERS 1 ETH OUTPUT TRANSFERS 29

---

## LAST 12 MONTHS

TOTAL TRANSACTIONS 30

---

TOTAL ETH TRANSFERS 30

---

TURNOVER 1.958981 ETH  
\$6 829.19

---

 TOTAL ETH INPUT 1.948981 ETH \$6 794.32  TOTAL ETH OUTPUT 0.01 ETH \$34.86

---

AVG ETH INPUT 0.64966 ETH \$2 264.77 AVG ETH OUTPUT 0.000357 ETH \$1.25

---

LARGEST 1.009431 ETH \$3 518.97 LARGEST 0.01 ETH \$34.86

---

SMALLEST 0.0001 ETH \$0.35 SMALLEST 0 ETH \$0.00

---

ETH INPUT TRANSFERS 1 ETH OUTPUT TRANSFERS 29

---

## FIRST INCOMING TRANSACTION

TRANSACTION HASH [e10ff2e2ba0530676ab8388a32308f587cd68b48f2d58e552f3634008552c437](#)

---

BLOCK TIME 03.09.2021 20:27:19

---

BLOCK HEIGHT 13154901

---

TRANSACTION AMOUNT 0.93945 ETH

---

TRANSACTION USD VALUE \$3 687.44



#### FIRST OUTGOING TRANSACTION

---

TRANSACTION HASH	6458b59f9fe0921cf433f136a87842c85fb99f6d276d4d5a6429e245e4095666
------------------	--

---

BLOCK TIME	03.09.2021 20:40:29
------------	---------------------

---

BLOCK HEIGHT	13154965
--------------	----------

---

TRANSACTION AMOUNT	0.01 ETH
--------------------	----------

---

TRANSACTION USD VALUE	\$39.19
-----------------------	---------

#### LAST INCOMING TRANSACTION

---

TRANSACTION HASH	002d2670b967211b41f30084f0f1daa6c59486ccfad60de49647976c7a45307
------------------	---

---

BLOCK TIME	04.09.2021 07:50:57
------------	---------------------

---

BLOCK HEIGHT	13157971
--------------	----------

---

TRANSACTION AMOUNT	0.0001 ETH
--------------------	------------

---

TRANSACTION USD VALUE	\$0.39
-----------------------	--------

#### LAST OUTGOING TRANSACTION

---

TRANSACTION HASH	6ac8c30cba76e58ed875478877250e3a672a887807d0694107d75223c65d5375
------------------	--

---

BLOCK TIME	04.09.2021 01:00:42
------------	---------------------

---

BLOCK HEIGHT	13156154
--------------	----------

---

TRANSACTION AMOUNT	0 ETH
--------------------	-------

---

TRANSACTION USD VALUE	\$0.00
-----------------------	--------

LAST 24 HOURS ACTIVITY

---

INFLOW

0 ETH

---

OUTFLOW

0 ETH

---

AVERAGE INFLOW

0 ETH

---

AVERAGE OUTFLOW

0 ETH

## 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](mailto:report@coinfirm.com).

**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) is 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) is 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) is 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.