Chainalysis

Chainalysis Cryptocurrency Fundamentals Certification Reference Guide

Origin of Bitcoin

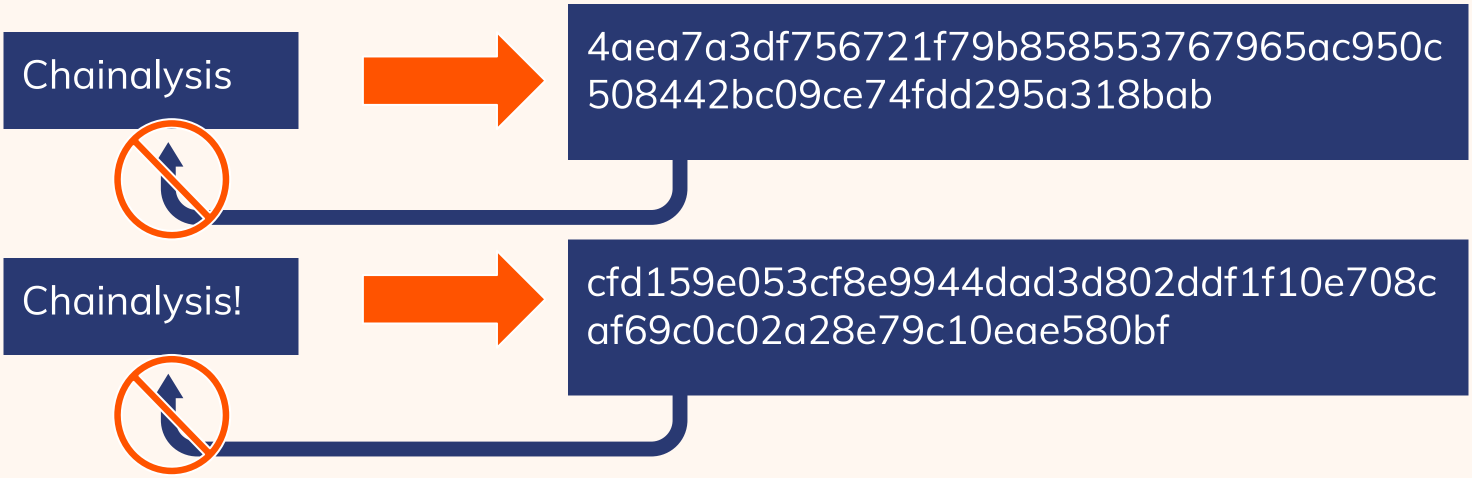
- The original Bitcoin white paper was published on October 31, 2008 under the pseudonym "Satoshi Nakamoto".
- "A purely **P2P** version of electronic cash [to] allow **online payments** to be sent **directly** from one party to another **without** going through a **financial institution**."
- The first block was produced on January 3, 2009.

Bitcoin Quick Facts

- Limited to 21 Million
- Utilizes the UTXO transaction model
- Distributed open/public ledger (the " Bitcoin blockchain")
- Pseudo-anonymous
- Trust through **cryptography**: mathematics concerned with data integrity and secure communications:
  - Secures the ledger - very difficult for 'bad' actors to make changes.
  - Makes ledger entries easily verifiable.
  - Prevents counterfeiting - creates **digital scarcity:**
    - Can only create bitcoin in very specific circumstances.
    - Cannot spend bitcoin received more than once.

Hashing: One-way, deterministic, unique

- Hashing is a mathematical function where any length input gives a fixed length output which is the same every time.
- Easy to go from input -> output - **not** output -> input: it's a one way street.



Chainalysis

4aea7a3df756721f79b858553767965ac950c508442bc09ce74fdd295a318bab

Chainalysis!

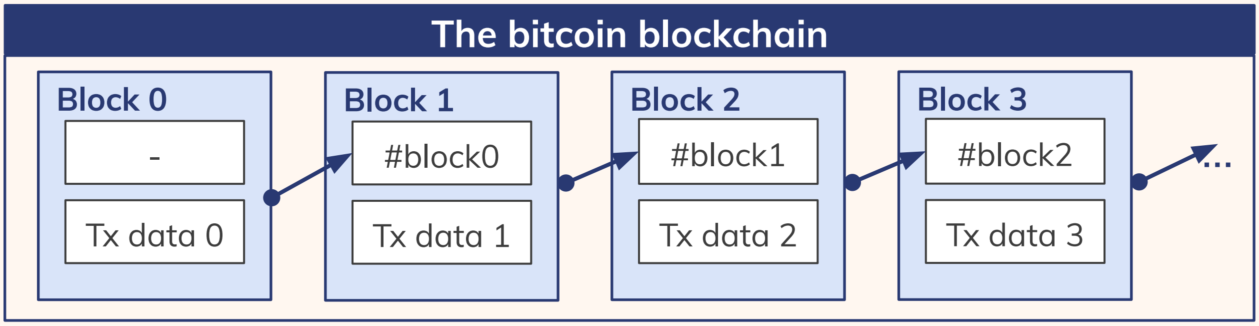
cfd159e053cf8e9944dad3d802ddf1f10e708caf69c0c02a28e79c10eae580bf

Small change to input = complete change in output; no link input to output

Use	Detail
Address generation	Public key hashed to give a more user friendly public identifier and to add an extra layer of security.
Mining (Proof of Work)	Computational guessing game to produce a hash below a target value.
Linking blocks in the chain	Hash of previous block included in the data of the next one - changing the previous one makes the next invalid.
Creating unique IDs	Block data hashed = block ID Transaction data hashed = transaction ID

Blockchain: Chained Ledger Entries

- Satoshi proposed a ledger system that would come to be known as '**blockchain**'.
- **Blockchain = a way to store data in sequence: reliable decentralised ledger.**
    - Data is **compiled** together into blocks, then **hashed** together.
    - For Bitcoin, that data = transactions.
    - Each new block contains hash of previous block creating a chain.
        - **Tx data 2 + #block1** => **#block2**



The bitcoin blockchain

Block 0: - / Tx data 0

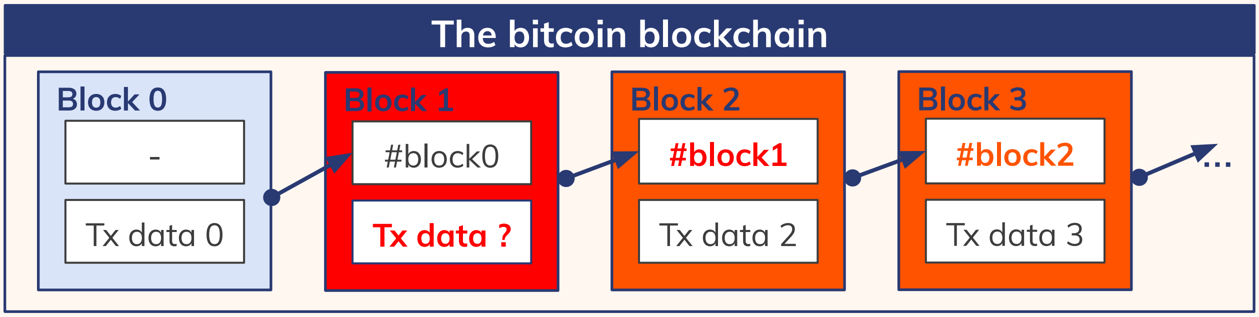
Block 1: #block0 / Tx data 1

Block 2: #block1 / Tx data 2

Block 3: #block2 / Tx data 3

...

- Any change in block data changes the block hash.
- The block hash is a part of the next block - so this block becomes invalid. Every subsequent block is no longer valid.



The bitcoin blockchain

Block 0: - / Tx data 0

Block 1: #block0 / Tx data ?

Block 2: #block1 / Tx data 2

Block 3: #block2 / Tx data 3

...

- Anyone can choose to run software and compete to win the right to update the ledger. This computational guessing game requires **energy** to be expended which participants must pay for.
- These bitcoin **miners** - are trying to find a specific hash output below a set value, using their block data as an input. This is **proof of work** mining - they must prove to the network that they have a solution to the puzzle. The only way to get the solution is to expend energy - i.e. doing work!

Bitcoin Monetary Policy and Protocols

2009-2012

- Block reward = 50 BTC

2012-2016

- Block reward = 25 BTC

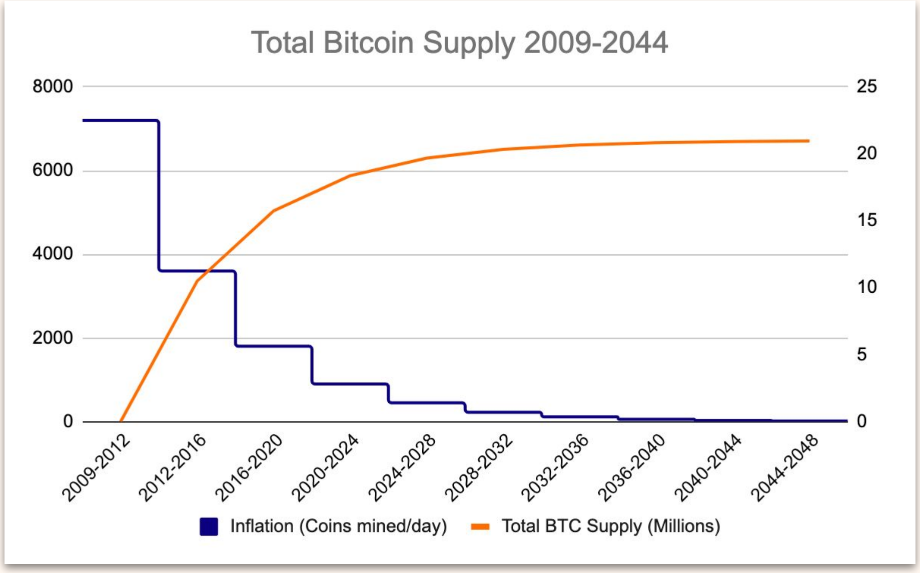
2016-2020

- Block reward = 12.5 BTC

2020-2024

- Block reward = 6.25 BTC

Total supply = 21 million
99.9 % available by 2044



Bitcoin protocol and the Bitcoin network

Protocol defines the **rules governing the network** including:

- How transactions are validated.
- How new ledger entries (blocks) are validated.
- Rate of issuance of new bitcoin (reward to miners/monetary policy).

All network participants run software enforcing the same rules and actively disconnect from participants (nodes) that do not follow the rules

- Nodes are equal peers with **different** functions.
  - Light node - No copy of ledger
  - Full - Own full copy of ledger
  - Mining - Own copy of ledger, and creates blocks

Wallets, Keys, Addresses

Custodial

Hosted Wallet (bank/safety deposit)

- Company controls private keys
- They control your bitcoin
- They choose which wallet they want

Web Interface
Mobile Interface

Non-Custodial

Private Wallet (under the mattress)

- Individual holds private keys
- You control your bitcoin

Web Wallet
Mobile Wallet
Software Wallet

Hot storage

Cold Storage

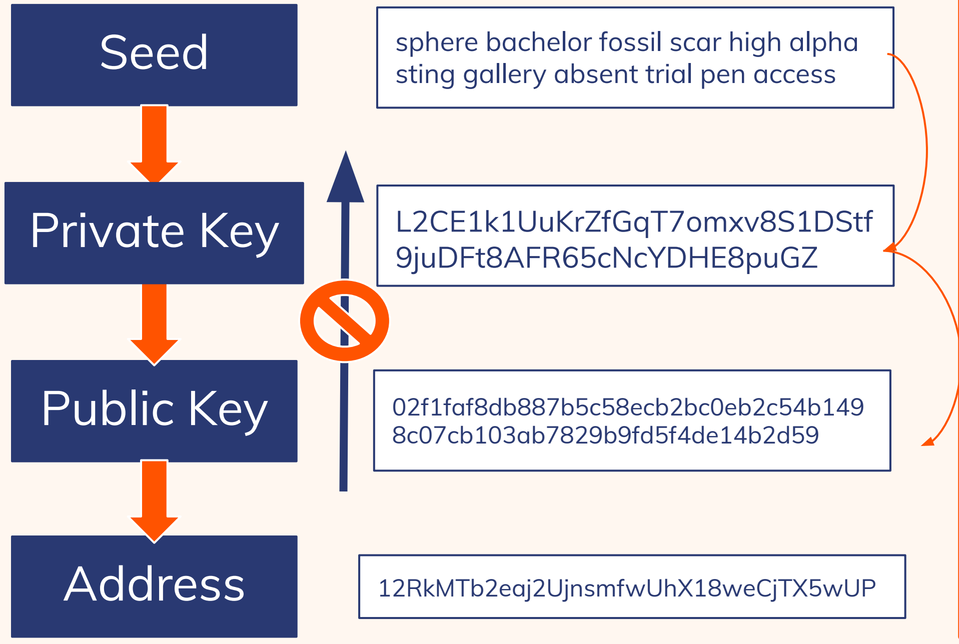
Hardware Wallet
Paper wallet

Different companies provide different UI, support, security and functionality

	Definition	Use
Wallet	Software running the bitcoin protocol; enables communication with the network; generates, stores and manages private keys.	Access the Bitcoin network; construct transactions and enable sending and receiving.
Seed Phrase	Mnemonic 12-24 word phrase used to generate private keys in a wallet.	A backup to generate identical private keys in different wallet.
Private Key	Generates an address you can send funds to, and unlock funds received at that address.	Proves ownership of linked address - enables 'spending'.
Address	A unique identifier where cryptocurrency can be sent. Privacy best practice = use once	Viewed on public ledger to see associated transaction history.

A wallet is more like a **keychain** than a store of coins; it manages **private keys**.
Balances are calculated by referring to the blockchain. Bitcoin are **not** stored in a wallet

Public / Private key cryptography



sphere bachelor fossil scar high alpha sting gallery absent trial pen access

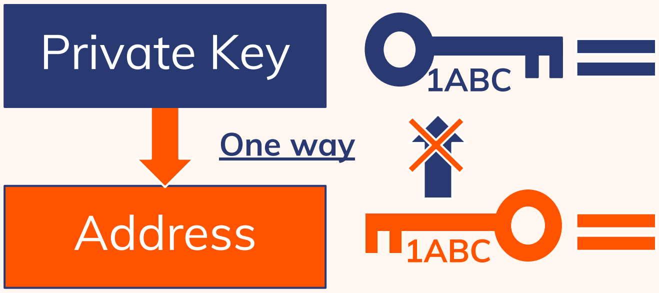
L2CE1k1UuKrZfGqT7omxv8S1DStf 9juDFt8AFR65cNcYDHE8puGZ

02f1faf8db887b5c58ecb2bc0eb2c54b149 8c07cb103ab7829b9fd5f4de14b2d59

12RkMTb2eaj2UjnsmfwUhX18weCjTX5wUP

Each cryptographically linked to preceding form - easy to calculate: **Not possible to guess the private key from seeing its corresponding address or public key.**

Hash function used to produce address from public key

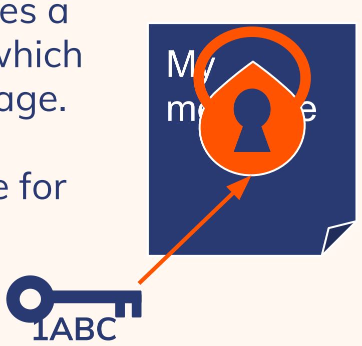


The way you prove you control the identity - e.g. email account password

The way you share your identity with the world - e.g. email address.

Private key produces a **digital signature** which encrypts the message.

Signature is unique for each message.



Public key decrypts the message.

Sent with encrypted message for others to check validity of the signature.

Control of private key means you control the identity ‘1ABC’.

Address Types

Starts with	Technical name	Date activated	Purpose
1...	Pay to public key hash (P2PKH)	Jan.3, 2009	Original address type
3...	Pay to script hash (P2SH)	Apr. 1, 2012	Enables more complex scripting and efficient use of block space.
bc1...	bech32	Aug. 24, 2017	Even more efficient use of space in a block, thus lower fees. Case insensitive

From Transaction to Block

1 Transaction constructed, signed & broadcast to Bitcoin network. Sender will pay a fee for their transaction.

2 All nodes first validate transaction, then add to their mempool and broadcast to connected nodes. Until transaction is in the blockchain it is 'unconfirmed'.

3 Miner compiles candidate block (including your transaction).

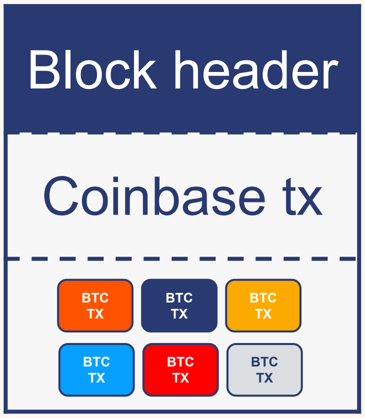
4 Miner competes to guess proof of work solution for their block.

5 Miner finds solution - broadcasts block to the network.

6 Nodes validate block, update their ledger copy.

7 As all nodes update their ledger, your transaction is confirmed. As more blocks are added on top of this one the transaction has more confirmations - there is greater certainty that the ledger will not be changed.

Proof of Work



Block header data + Nonce = Hashed value

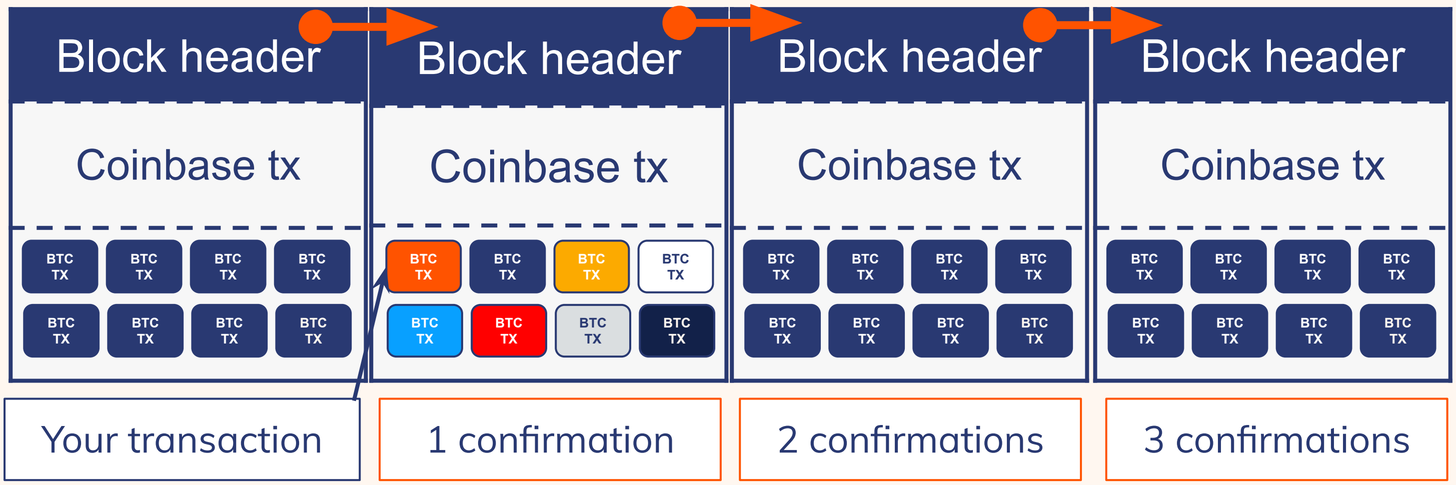
Nonce	Hashed value
0	e3b0c...4f855
1	56b8...394bf
n	00000000....

- Block header is constant, **nonce** is varied to give a different hash value.
- Miners create different blocks- they're all looking for "n" for their own block.

Hash less than target value = a valid block e.g. less than 000000000000000000092...

Immutability

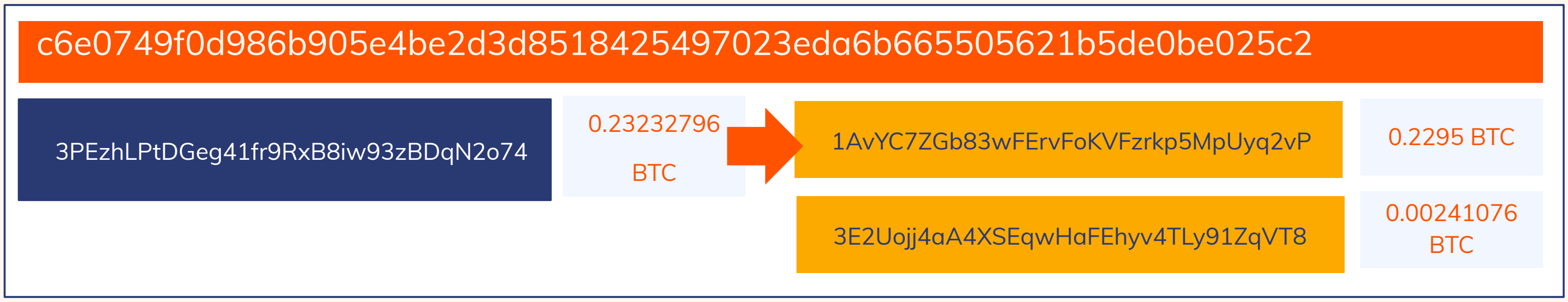
- More confirmations = more computational power to change the block containing your transaction and every block on top of it = more certain. 6 confirmations considered "immutable"



Block Explorers

Transaction contains:

1. **Transaction ID / Hash**: unique identifier in the Bitcoin blockchain
2. **INPUTS**: source of bitcoins (one or more addresses)
3. **OUTPUTS**: destination of bitcoins (one or more addresses)



c6e0749f0d986b905e4be2d3d8518425497023eda6b665505621b5de0be025c2

3PEzhLPtDGeg41fr9RxB8iw93zBDqN2o74

0.23232796 BTC

1AvYC7ZGb83wFErvFoKVFzrkp5MpUyq2vP

0.2295 BTC

3E2Uojj4aA4XSEqwHaFEhyv4TLy91ZqVT8

0.00241076 BTC

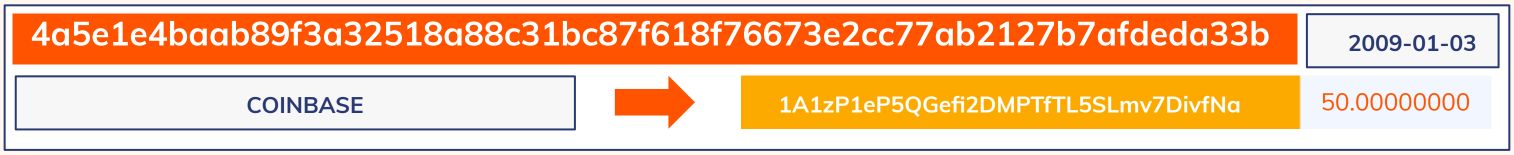
Public blockchains provide:

1. TIME OF TRANSACTION
2. AMOUNT TRANSACTED (including fees)
3. ADDRESSES INVOLVED

? They do not provide the identity of an individual or entity.

Unspent Transaction Output (UTXO) Model

- Inputs to each transaction are unspent records of transaction outputs forming a **chain** of transactions that **you can track** forwards / backward.
- The record of funds sent to an address **do not merge** together.
- When spending a transaction output, ‘leftover’ bitcoin are returned to an address from the sender’s wallet as ‘change’.
- The Coinbase transaction - the block reward and transaction fees transferred to the successful miner of a specific block - is the first in a sequence of outputs.

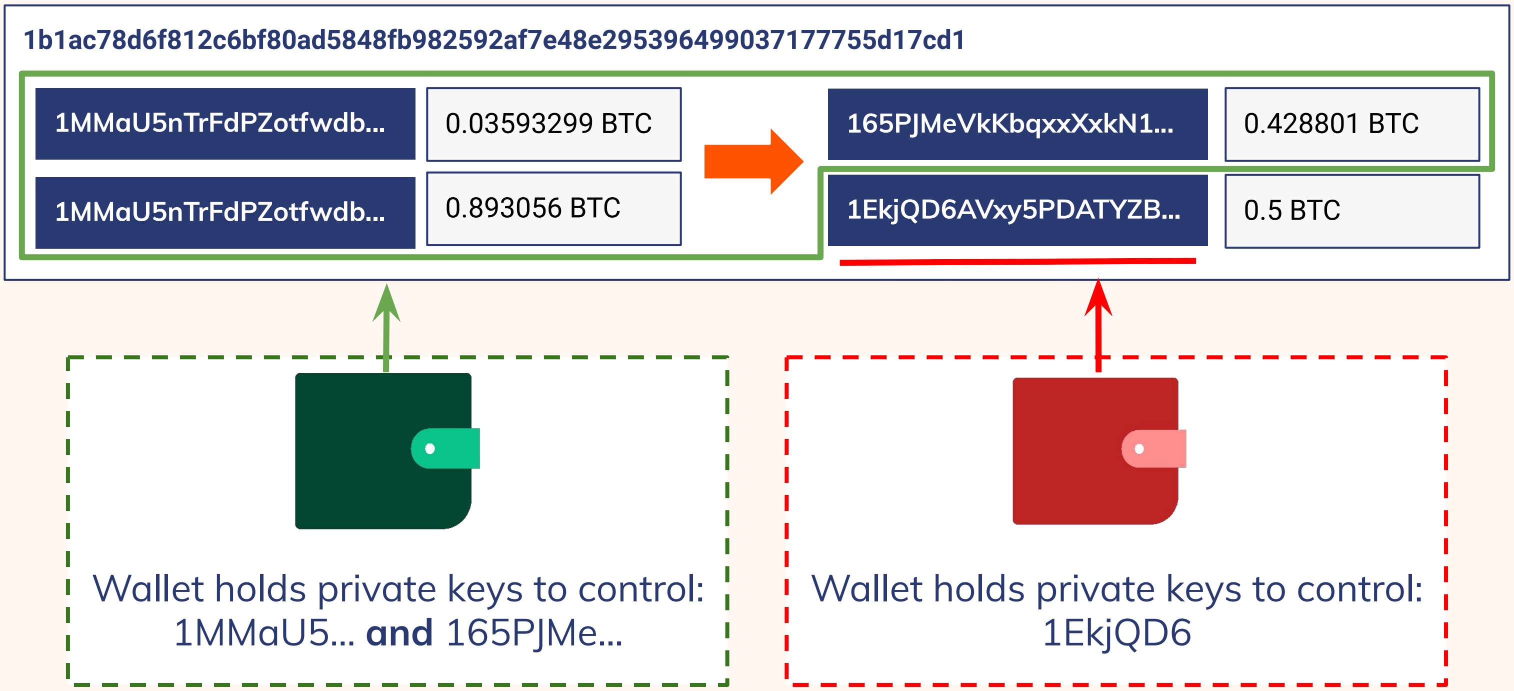


4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

2009-01-03

COINBASE → 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa 50.00000000

Change



1b1ac78d6f812c6bf80ad5848fb982592af7e48e2953964990371777755d17cd1

1MMaU5nTrFdPZotfwdb... 0.03593299 BTC

1MMaU5nTrFdPZotfwdb... 0.893056 BTC

→

165PJMeVkKbqxxXxkN1... 0.428801 BTC

1EkjQD6AVxy5PDATYZB... 0.5 BTC

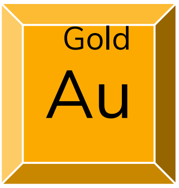
Wallet holds private keys to control: 1MMaU5... **and** 165PJMe...

Wallet holds private keys to control: 1EkjQD6

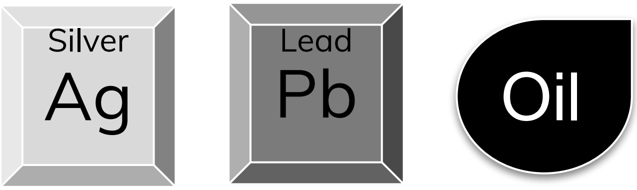
Change is not labelled on the blockchain - but analysis can help identification. Do you follow the payment or do you follow the change?

Alternative Cryptocurrencies

If Bitcoin is Digital Gold:



Altcoins are Digital...



Huge number of alternatives, varying wildly in value:

- Alternative use cases
- Different value - dependent on supply and demand
- Different technology, protocol, ledger system, addresses
- Variety of different tokens and use cases can be a regulatory challenge

Categories

Native tokens

- **Own blockchain**
  - Bitcoin, Ethereum, Litecoin, Ripple
- **Forked blockchain**
  - Split from a previous chain due to change in ‘rules’ - partial shared tx history with original token.
    - Bitcoin Cash, Ethereum Classic

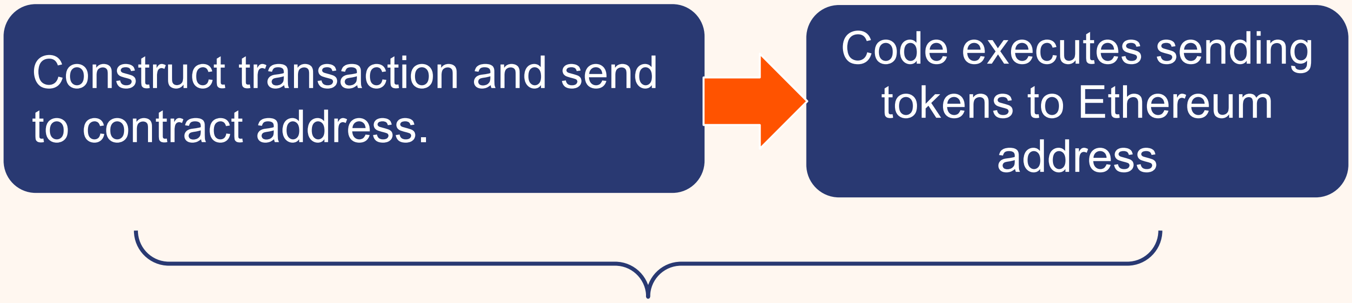
Non-native tokens - built on top of another blockchain

- Stablecoins
- Initial Coin Offering (ICO) Tokens
- ERC-20 / ERC-721

Smart Contracts

Code recorded on the blockchain: it executes when certain conditions are met - “**if this** happens, **then that** happens…” - They execute a predefined set of terms automatically that are trackable and irreversible.

- Deterministic digital agreement, transparent to all.
- Insert coin -> receive soda / Deposit ETH -> receive tokens



Construct transaction and send to contract address.

Code executes sending tokens to Ethereum address

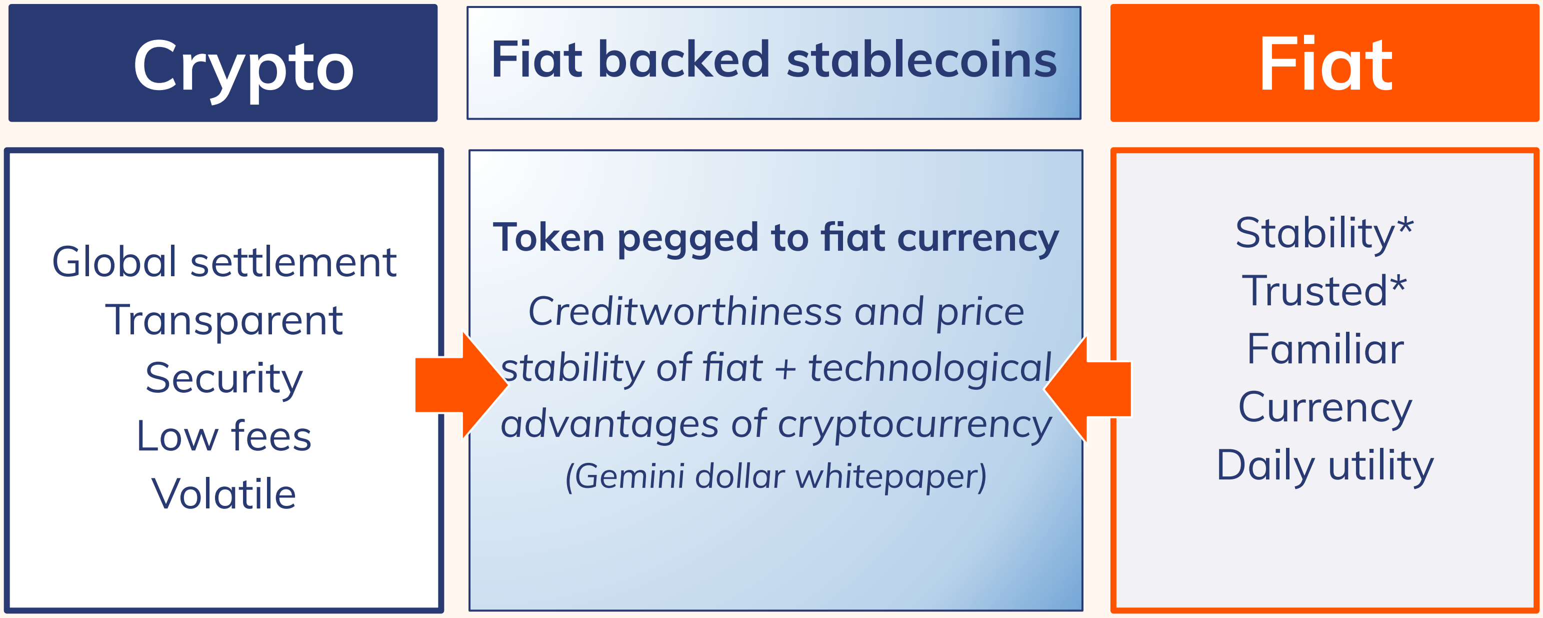
Process recorded in the Ethereum blockchain held by all nodes

Tokens

	Description	Example use cases
Utility Tokens	Access to a service or user experience	Basic Attention Token (BAT) reimagines user / advertiser engagement on Brave browser.
Security Tokens*	Investments - promise of future dividends	DAO - token grants holder share of profits from investment fund.
Currency / Payment tokens	Facilitate digital payment process	Stablecoins: USDT, GUSD - create stable, secure and transparent digital asset.

Tokens stored at an address on the ‘host’ blockchain - 1 address can store many tokens

Stable Coins



Crypto

Global settlement
Transparent
Security
Low fees
Volatile

Fiat backed stablecoins

Token pegged to fiat currency

Creditworthiness and price stability of fiat + technological advantages of cryptocurrency

(Gemini dollar whitepaper)

Fiat

Stability*
Trusted*
Familiar
Currency
Daily utility

Privacy Coins

	Privacy type	Other details
Monero	Mandatory	Available on a limited number of exchanges - Fiat/Monero available at Local Monero P2P Offboarded by some exchanges due to criminal use
ZCash	Transparent or shielded	Aim to 'empower everyone with economic freedom and opportunity' - supported by NYDFS regulated exchanges like Gemini. Enable commercial privacy.

Industry Typologies

Name	Description
Exchange	Online service for buying, selling, and trading cryptocurrency
Merchant Service	Financial services authorized to accept customer payments on behalf of a business. Known as payment gateways or payment processors.
Hosted Wallet	Alternative to individually controlled wallets. Easier to use, and potentially more secure. Risky if you don't choose a good one.
Miners	Mine blocks and include transactions - keep Bitcoin running. Located near source of cheap electricity. Can combine resource in pools.
Crypto Kiosks	Convert cash into cryptocurrency & vice versa, (also called crypto ATMs)

Risky Typologies

Name	Description
Darknet Markets	Black markets for drugs, stolen card data, weapons, etc
Ransomware	Malicious software that encrypts computer files for ransom
Stolen Funds	Cryptocurrency which has been stolen in exchange hacks
Scams	Bad actors trick victims into sending them cryptocurrency or giving them their account credentials
Extremist Financing	Fundraising campaigns soliciting cryptocurrency
Sanctions	OFAC has sanctioned multiple crypto addresses associated with various entities

Regulation

Financial Action Task Force (FATF)	Intergovernmental standards setting body
	Assists in defining AML / CTF policy globally through recommendations
	Evaluates the efficacy of financial regulation & AML / CTF policy implementation
	June 2019 guidance for a risk based approach to/for Virtual Asset Service Providers + subsequent 12 / 24 month reviews

FATF’s Approach to Virtual Assets (VAs)

Defines Virtual Asset Service Provider (VASP)	Businesses that exchange, transfer or custody VAs. E.g. Exchanges, hosted wallets, ICOs & others (not private persons’ wallet).
Licensing and Registration for VASPs	Still in process of being applied in many jurisdictions
Blockchain analysis & automated transaction monitoring essential	Monitoring to be carried out continuously and triggered by specific transactions. Enhanced monitoring for higher risk situations - going beyond the immediate transaction (tracking on the blockchain).
Travel Rule	VASP must obtain and hold details of sender and recipient for transactions over 1000 USD / 1000 EUR and send this to any VASP counterparty.

Blockchain Analysis

Aims

- Imposes structure onto the blockchain, collapsing addresses into larger entities.
- View transactions at an entity to entity level, not an address to address level.
- Provides context to transactions through identifying services and illicit actors.
- Visualises entity transactions to facilitate tracking and analysis.

Application

Crypto Businesses	Develop compliance policies. Monitor transactions for risky counterparties.
Banks	Benchmark and monitor services seeking banking support.
Government	Investigate criminal activity. Supervise licensing / registration regulatory regime

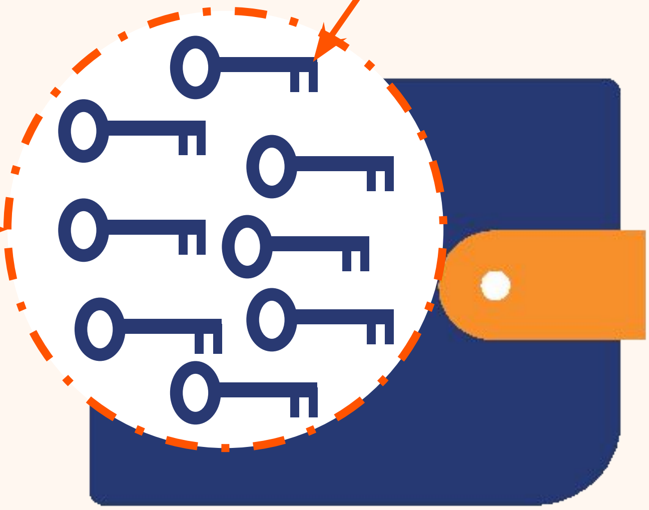
Blockchain Analysis

16W1ZmJjnp5y7aExjsChxq2djeBWHkjKtt
1NRM51564QmvN89wopQn76UbaVgqZ86EK1
1HdB81pyZRzTQABRy2G7ot5v6QkEKHMeEo
1HV9hPijND3y3gEtQWoSCtJKHcdBEGZC8p
1MEEYFiJ5dNq8C7MrobWmn6uNGCyJqx8tu
13LvhDmTqHSYYdgxoNZmtL2xcTnfY8X88Y
1HrpwsTZFKiPf9hHVhh5kKy1ZVpkcZb2Wu
1JfGSdyAngEb4ou9pEL1zXrzmrhFbbfQhA
1KGY8rsoufBQbG3rGXpEvo7P6j2sCeazPh
16fY2QXhhBasn3KuSuU8WZb8vSiQvYjg5w

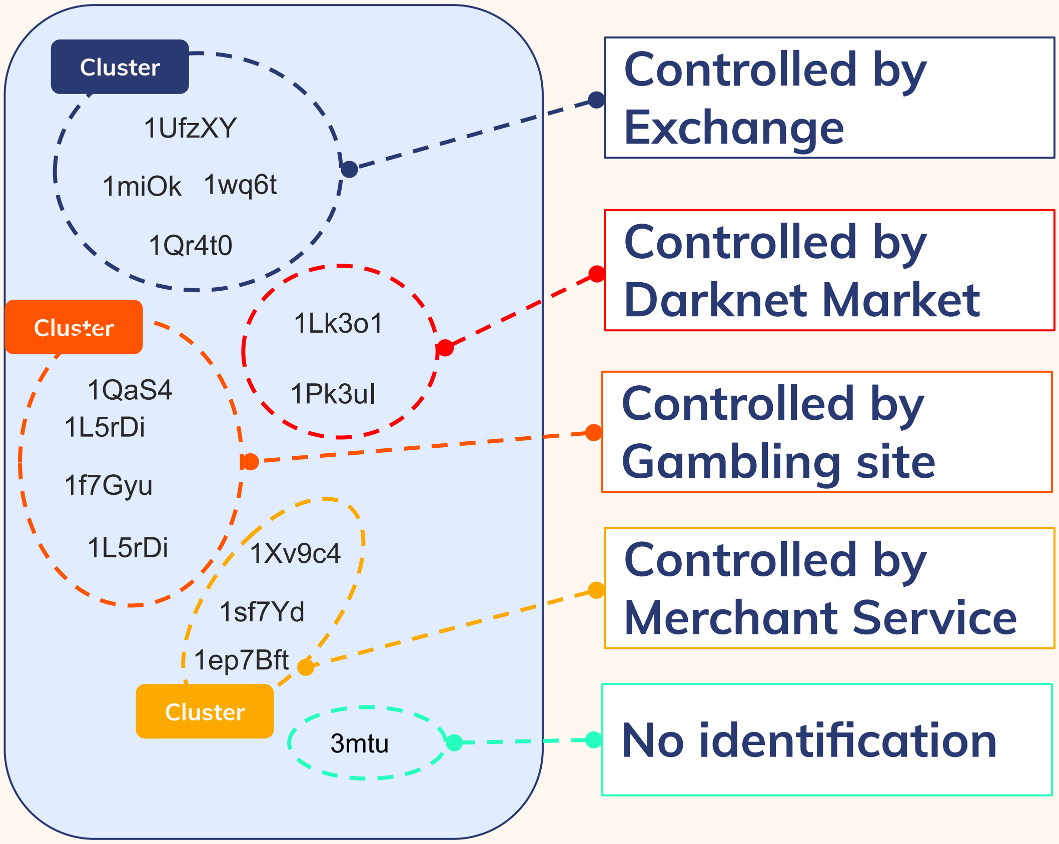
1BoH55aULHZ28h5q7YUHu6yr7fbvmNgGcG

Payment going to a different wallet

1KAao9J5ErbmeJm6FTRVrRSunmYPTpcQa2



Co-spending: a single wallet using multiple UTXOs as inputs to a transaction; all controlled by private keys **in the same wallet**



Controlled by Exchange

Controlled by Darknet Market

Controlled by Gambling site

Controlled by Merchant Service

No identification

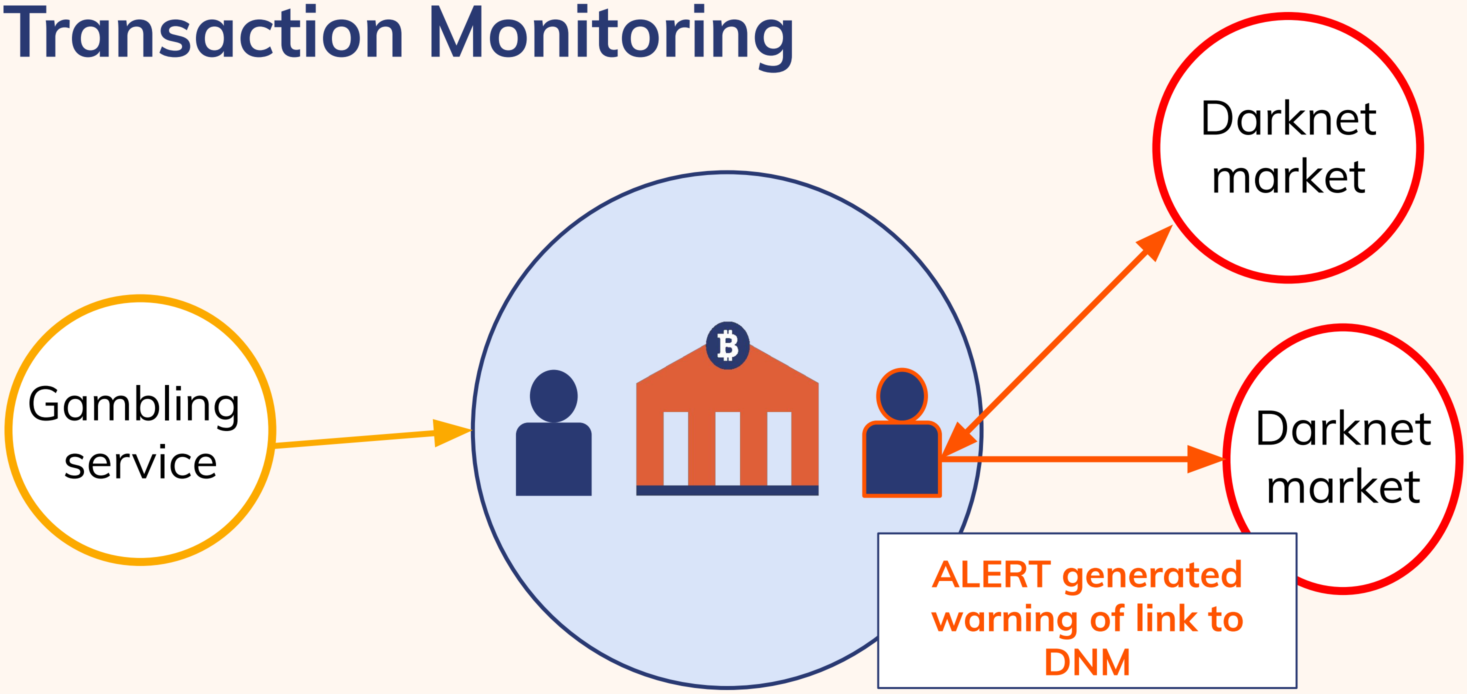
Identification

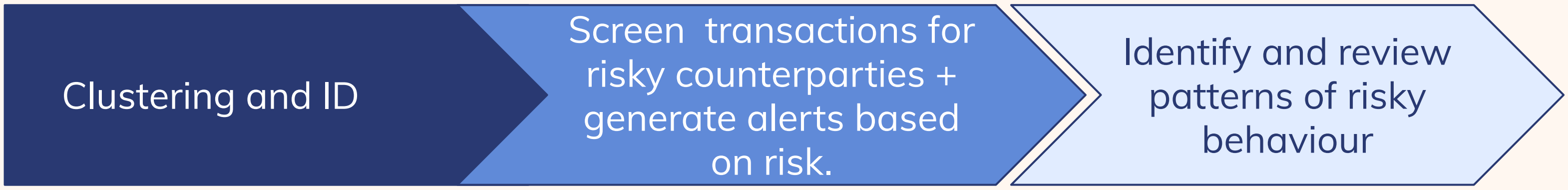
Deposits and withdrawals to services

Research

Data analytics and heuristics

Transaction Monitoring




Clustering and ID
Screen transactions for risky counterparties + generate alerts based on risk.
Identify and review patterns of risky behaviour

Transactions sent to a service complete before the receiving exchange can apply their transaction monitoring solution: **cannot refuse a risky deposit.**

- Can decide whether to credit the user account.
- The risky exposure will still show up - you can't rewrite the blockchain!

Transactions sent from a service are **constructed by the service** and can be reviewed before sending: **potential to stop an *identified* risky withdrawal.**

- Only applies if the exposure to a risky counterparty is identified at the time of the transaction.

Alert thresholds exercise

You're part of a new crypto exchange supporting bitcoin only.

- Consider the following risk categories:
    - Ransomware, Mixers, Peer2Peer exchange
- For each category decide what your threshold for being alerted to your customer sending / receiving **directly** from/to bitcoin addresses identified as being part of these categories.
- Consider whether the alert needs to be generated when funds are sent / received (or both) from the counterparty.
- What action might you take as a result of any alerts? *Send user an email asking for more information? Offboard from your platform? Monitor for repeat alerts?*

Category	Direction (Sent / Received or both)	Threshold value for alert	Compliance action Offboard? Question? Warning? Report?
Terrorist finance (example only)	Sending or receiving	0+ USD	Report to FIU Offboard depending on FIU guidance
Ransomware			
Mixers			
P2P			

Glossary of terms

5AMLD

Fifth EU Anti-Money Laundering Directive. Prevents the financial system being used for the funding of criminal activities and strengthens transparency rules to prevent large-scale concealment of funds.

Address

A digital destination used to send and receive cryptocurrency funds. It is similar to a physical house address or an email address, however, cryptocurrency wallets often generate many addresses. A Bitcoin address consists of 26-35 alphanumeric characters.

Block

An entry of the cryptocurrency transactions that have been made in a certain time frame batched together. A new block is validated approximately every 10 minutes on the Bitcoin network and becomes part of the blockchain. The blockchain is a sequence of connected data blocks.

Block Explorer

A website for viewing public blockchains and checking transactions that provides information on any transactions and blocks, including their status and confirmation time. Example: https://www.blockchain.com/explorer.

Cluster

A collection of cryptocurrency addresses that Chainalysis has identified to be controlled by one entity. This is a crucial aspect of blockchain analysis.

Cold Wallet

A type of wallet that is not connected to the internet. This is also referred to as cold storage.

Counterparty

The other party that participates in a cryptocurrency transaction.

Custodial Wallet

Describes where a company or organization holds private keys controlling cryptocurrency on behalf of their users. The user base is not in control of the wallet software and must request the company to manage withdrawals from their accounts.

FATF

Financial Action Task Force. Global money laundering and terrorist financing intergovernmental organization, that sets international standards guidance which is then implemented and enforced by member States.

FATF Travel Rule

A FATF regulation that requires cryptocurrency exchanges to verify their customers' identities, identify the original parties and beneficiaries of the direct transfer between VASPs for 1000 USD/1000 EURO or higher and transmit that information to the counterparty VASP.

Hosted Wallet

A wallet that resides on a third-party service. The third-party service may hold both the user's private and public keys.

Hot Wallet

A wallet that resides on a device connected to the internet, like a desktop computer or smartphone.

Input

The cryptocurrency address from which funds were sent (the source of the coins in a single transaction). For UTXO coins (see below) an input is a reference to an output from a previous transaction.

Mempool

The space where nodes store validated transactions prior to their inclusion in a block.

Mining

The process by which transactions are validated and issued on the blockchain network. Miners receive a reward of cryptocurrency where they successfully add a block to the blockchain.

Mining Pool

A grouping of resources by miners who share their processing power over a network, to split the block-reward according to the amount of work they contributed to solving a block.

Node

A participant in the blockchain network. There are numerous types of nodes that have different functions on varying blockchains, including (but not limited to) full nodes, mining nodes, lightweight nodes.

Output

The cryptocurrency destination address(es) for funds; i.e. where funds are being sent. There can be multiple inputs and outputs for a single transaction.

Paper Wallet

A type of cold storage wallet where private keys are printed on a piece of paper, written down, or exist on another physical medium.

Private Key

A secret alphanumeric string that allows the user to access the funds at a single corresponding address. Wallets contain one or more private keys.

Public Key

An alphanumeric string that is used to derive an address. The public key is only publicly known if currency has been spent from its corresponding address.

Stablecoin

A cryptocurrency that attempts to minimize price volatility by pegging the coin to a cryptocurrency, fiat money, exchange-traded commodities, or through an algorithmic process designed to increase / decrease the supply of tokens to stabilize the price.

Seed Phrase

Also known as mnemonic, 12-24 word sequence which can be used as the deterministic backup for a wallet - enables recreation of the private keys in another compatible wallet.

Transaction

A transaction consists of one or more fund transfers. A bitcoin transaction comprises: a unique transaction ID (the transaction hash); input(s), which are the source of the coins; and output(s), which are the destinations of the coins.

Transaction Hash

Also known as a transaction ID, the transaction hash is a unique identifier of a transaction.

UTXO

An acronym for Unspent Transaction Output. UTXO is used to describe the transaction model used by most blockchains. In the UTXO model, you spend previously unspent chunks of cryptocurrency.

VASP

An acronym for Virtual Asset Service Provider. VASP is the terminology used by regulators to identify business models operating with crypto currencies that fall under their jurisdiction.

Wallet

A software program that generates and stores a user’s addresses and private keys. It is used to send and receive cryptocurrency and monitor balances.

Chainalysis

Chainalysis Cryptocurrency Fundamentals Certification Reference Guide

Exercise & Exam Details Student Notes

CCFC Exercise Details

Exercise	Block ID, TX Hash, or Address
Block ID	Block #: 616362
Transaction Anatomy	2ae8a39f65fbbaf64988976993074569e34a896e040a93f0537715ccfd4ebbde
Source of Funds	D8888c8db50a491c8ca6aea7cc4b151a6a3995bf2f20f3619f3179951dbff5ed 5c76eb4dfb0941856a229833ef05b2f5c669dadc98ed2a34ea11974cacba9dc7
Block Explorer Analysis	e2b0536728ed6bbbf95d13ceb850f8d52fd56b1572a2660bdce9b97279c753a9
Binance Hack	e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea
Mixer	f7100a82279967efa504022cad3428a0be8cb3895f5c62a0e3840a54ed0a5550
Twitter	bc1qxy2kgdygjrsqtzq2n0yrf2493p83kkfjhx0wlh
Blockchain Analysis	14rKSWF7qQquUWHfmEHzCod71jB4SsVS6B

Exam Details

- 1.75 hours to complete the exam
- 80 multiple choice questions
- Passing score is 75%
- Open notes / open reference guide / open block-explorer

****Cannot work with anyone else****

	Website
Testing Platform	nexus.chainalysis.com
Exam Troubleshoot	https://support.skilljar.com/hc/en-us/articles/360033553054
Feedback	https://bit.ly/CCFCfeedback

Chainalysis certification exams must be taken by each individual
***no cooperation or working with others is allowed*.**
Chainalysis will review exam results prior to awarding certification to each individual.

Student Notes

Student Notes

Student Notes

Student Notes

Chainalysis