Introduction to Virtual Assets

Exercise 1

- In your groups discuss your understanding of virtual assets and detail two questions on something you don’t know which you would like input on. Seek to identify what you feel you do know as a group and use this to inform what questions you would like to ask.

At the end you will be asked to provide the two questions on a piece of paper which I will collect.

Introduction

- Natively digital assets which have a value associated to them for two main reasons:
  - Application
  - Supply and demand
- Many different types of asset, in some ways the stock market can be seen as a parallel.
- There are an infinite number of business ideas which can lead to a company being formed. If appropriate a legitimate company involved in almost any type of business, can seek to be listed on a stock market.
- As a result, the stock market contains entities involved in well known corporate activities, those serving niche businesses cases and everything in between.
- Cryptocurrency markets are the same. Many different ideas and business models reflected by a digital asset. Some compete with each other for market share and some are unique in their offering.

Introduction cont.

- The key metrics dictating use of cryptocurrency are liquidity and security.
- Security: To hold a significant value over the long term, an asset must be backed by sufficient security to prevent double spends or supply manipulation.
- Liquidity: An asset must be easy to buy and sell. This means many markets need to offer it as a trading pair.
- Bitcoin is currently the dominant cryptocurrency in respect of these features.

Networks

Two types of cryptocurrencies: Centralised (Recognised entity in control) and Decentralised (No entity in control).

Decentralised assets have two conceptual parts:

1) A Peer to Peer (P2P) network: P2P networks predominantly run over the internet. They use dedicated software to relay specific messages through a network of participants. Usually these are not regulated, anyone can join the network. This makes them difficult to censor.

2) Applications that run on this network. These are usually open source and free to run.

In summary applications generate data needed for transacting, while the network organizes and ensures the flow of information.

Networks cont.

Centralised cryptocurrencies have regulated network participants organising the flow of information. They can monitor and dictate what network traffic is deemed to be acceptable.

Often an exact mirror of the current financial system. Central bank digital currencies are an example of a centralised network.

There are obviously varying degrees of centralisation and this is something which is a constant discussion within the cryptocurrency environment.

Jargon: There is a lot of this!

- Crypto asset
- Cryptocurrency/ Cryptocurrencies
- Token
- Stablecoin
- Custodial/Non custodial
- VC: Virtual currency
- NFT: Non fungible token
- VA: Virtual asset
- VASP: Virtual Asset Service Provider
- CBDC: Central Bank Digital Currencies
- DEX: Decentralised Exchange
- DeFi: Decentralised Finance
- DAO: Decentralised Autonomous Organisation
- Dapp: Decentralised application

Need to know terminology

Blockchain: Database containing unique identifiers linking a new entry to the previous one. In Bitcoin it acts as a financial ledger (think bookkeeping)

Transaction Identifier (TXID): Unique transaction reference in the blockchain.

Network time: The Bitcoin blockchain operates on UTC only.

Wallets: Software that can be thought of as a bank in which you assets reside.

Addresses: Account numbers generated by the wallet software.

Inputs and outputs: Input are assets being spent and outputs are those created from the inputs.

Mining

Computationally intensive process for validating transactions, including them in the ledger, minting new assets and securing the network.

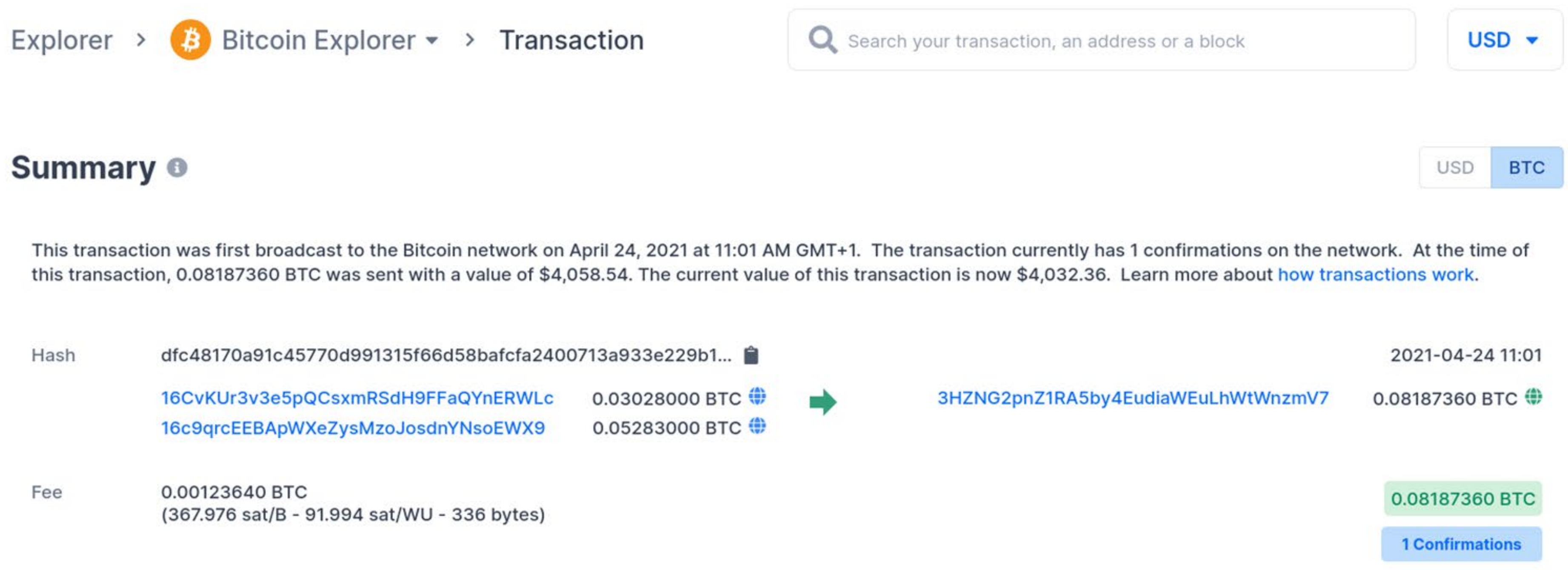
Financial incentives to complete this task. Miners get rewarded with fees and new asset issuance. If they act honestly and safeguard the network, then the asset will potentially appreciate in price. This will provide miners with further profits and an ongoing investment in sustaining the network.

As the network is decentralised a central entity cannot dictate who mines or gets rewarded for doing so. To mitigate this the Bitcoin protocol makes mining a free market, competitive environment. Anyone can compete and those who are most efficient will gain the greatest rewards.

"A good way to describe mining is like a giant competitive game of sudoku that resets every time someone finds a solution and whose difficulty automatically adjusts so that it takes approximately 10 minutes to find a solution. Imagine a giant sudoku puzzle, several thousand rows and columns in size. If I show you a completed puzzle you can verify it quite quickly. However, if the puzzle has a few squares filled and the rest are empty, it takes a lot of work to solve!

The difficulty of the sudoku can be adjusted by changing its size (more or fewer rows and columns), but it can still be verified quite easily even if it is very large. The "puzzle" used in bitcoin is based on a cryptographic hash and exhibits similar characteristics: it is asymmetrically hard to solve but easy to verify, and its difficulty can be adjusted."

- ***(Mastering Bitcoin: https://github.com/bitcoinbook/bitcoinbook/blob/develop/ch02.asciidoc)***



Explorer > Bitcoin Explorer > Transaction
Search your transaction, an address or a block
USD
USD BTC

Summary

This transaction was first broadcast to the Bitcoin network on April 24, 2021 at 11:01 AM GMT+1. The transaction currently has 1 confirmations on the network. At the time of this transaction, 0.08187360 BTC was sent with a value of $4,058.54. The current value of this transaction is now $4,032.36. Learn more about how transactions work.

Hash dfc48170a91c45770d991315f66d58bafcfa2400713a933e229b1... 2021-04-24 11:01

16CvKUr3v3e5pQCsxmRSdH9FFaQYnERWLc 0.03028000 BTC
16c9qrcEEBApWXeZysMzoJosdnYNsoEWX9 0.05283000 BTC

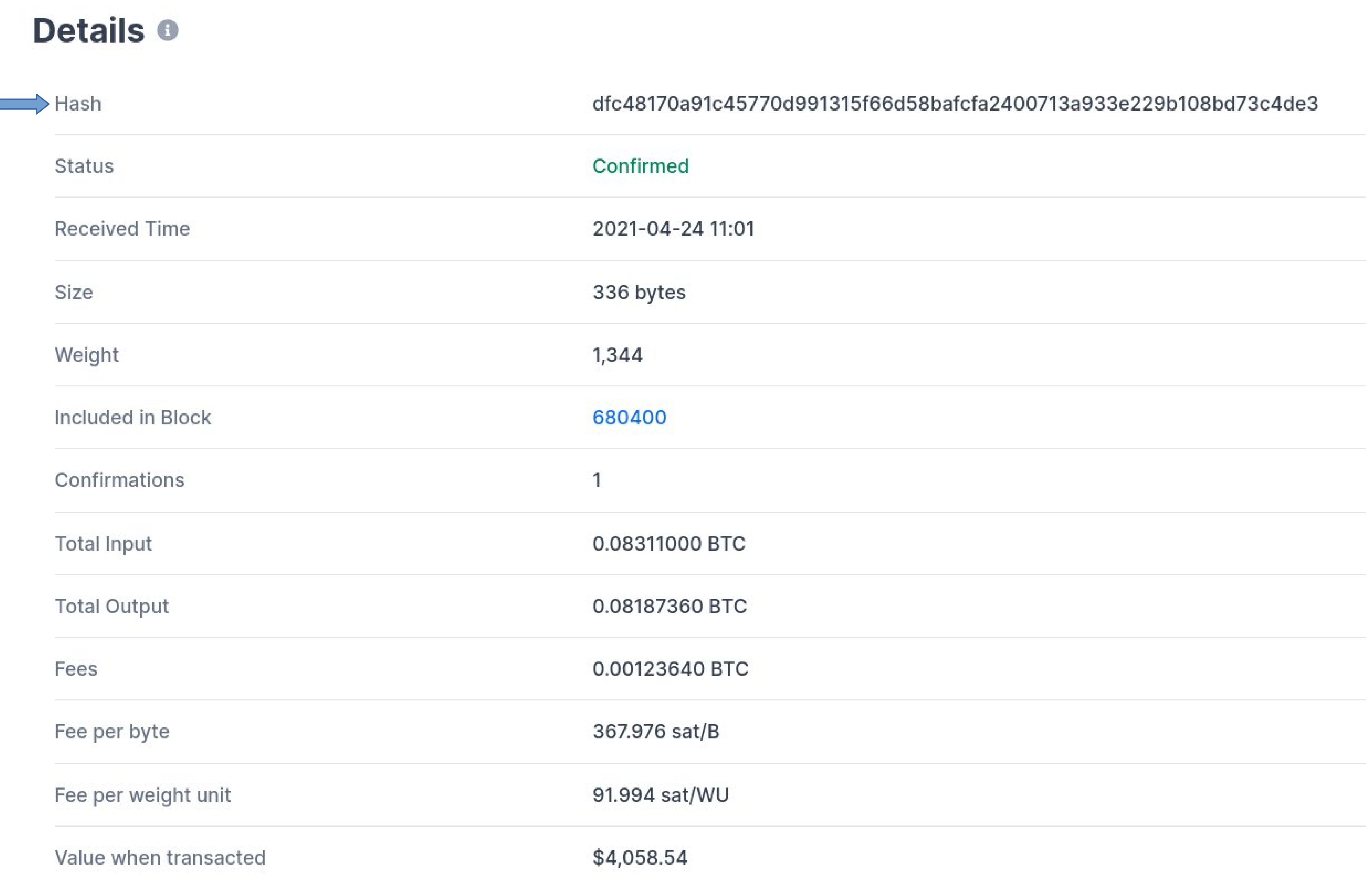
3HZNG2pnZ1RA5by4EudiaWEuLhWtWnzmV7 0.08187360 BTC

Fee 0.00123640 BTC
(367.976 sat/B - 91.994 sat/WU - 336 bytes)

0.08187360 BTC

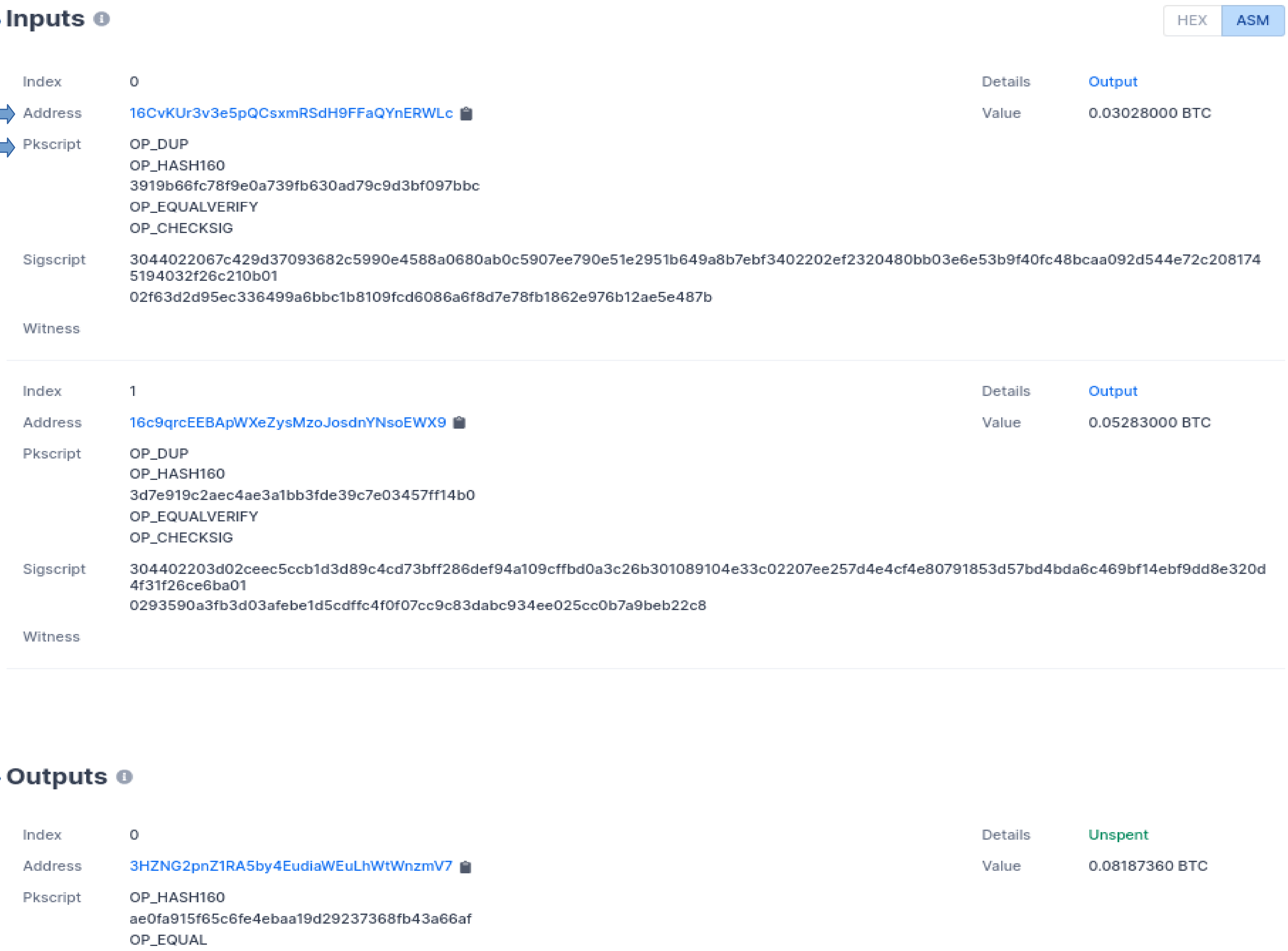
1 Confirmations

Anatomy of a Bitcoin transaction



Details

Hash	dfc48170a91c45770d991315f66d58bafcfa2400713a933e229b108bd73c4de3
Status	Confirmed
Received Time	2021-04-24 11:01
Size	336 bytes
Weight	1,344
Included in Block	680400
Confirmations	1
Total Input	0.08311000 BTC
Total Output	0.08187360 BTC
Fees	0.00123640 BTC
Fee per byte	367.976 sat/B
Fee per weight unit	91.994 sat/WU
Value when transacted	$4,058.54



Inputs

Index	0	Details	Output
Address	16CvKUr3v3e5pQCsxmRSdH9FFaQYnERWLc	Value	0.03028000 BTC
Pkscript	OP_DUP OP_HASH160 3919b66fc78f9e0a739fb630ad79c9d3bf097bbc OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	3044022067c429d37093682c5990e4588a0680ab0c5907ee790e51e2951b649a8b7ebf3402202ef2320480bb03e6e53b9f40fc48bcaa092d544e72c2081745194032f26c210b01 02f63d2d95ec336499a6bbc1b8109fcd6086a6f8d7e78fb1862e976b12ae5e487b		
Witness			

Index	1	Details	Output
Address	16c9qrcEEBApWXeZysMzoJosdnYNsoEWX9	Value	0.05283000 BTC
Pkscript	OP_DUP OP_HASH160 3d7e919c2aec4ae3a1bb3fde39c7e03457ff14b0 OP_EQUALVERIFY OP_CHECKSIG		
Sigscript	304402203d02ceec5ccb1d3d89c4cd73bff286def94a109cffbd0a3c26b301089104e33c02207ee257d4e4cf4e80791853d57bd4bda6c469bf14ebf9dd8e320d4f31f26ce6ba01 0293590a3fb3d03afebe1d5cdffc4f0f07cc9c83dabc934ee025cc0b7a9beb22c8		
Witness			

Outputs

Index	0	Details	Unspent
Address	3HZNG2pnZ1RA5by4EudiaWEuLhWtWnzmV7	Value	0.08187360 BTC
Pkscript	OP_HASH160 ae0fa915f65c6fe4ebaa19d29237368fb43a66af OP_EQUAL		

Ethereum: Key points

1. Ethereum utilise “accounts” as opposed to a UTXO model. This means one address can be used to complete all transactions. There is no separate change address or need to create a new address for every receipt.

2. Tokens created on the Ethereum protocol are not stored by holders in separate address types. They are credited to an Ethereum address.

3. Transaction fees are calculated using an element called “Gas”. The native Ethereum asset (ETH) is used to pay for fees.

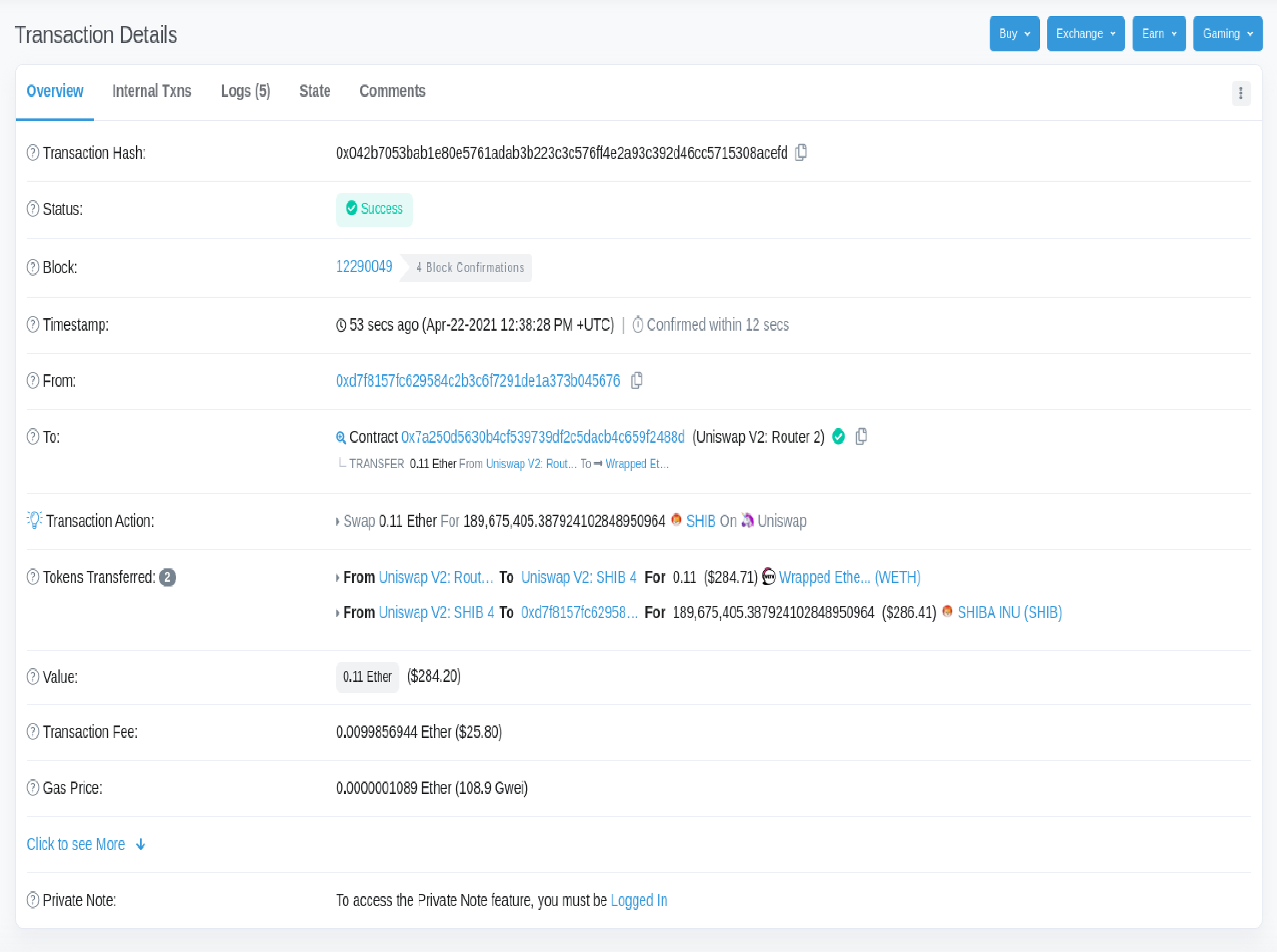
4. It is possible to utilise the transparent nature of many smart contracts to follow the route an asset has taken.

5. The more complex the execution of the transaction, the more Gas it consumes. This equates to higher fees being paid.

6. ETH on it’s own is not seen as a significant asset utilised by criminals.

7. It is however the main platform for stablecoins which have seen extensive use in money laundering. In particular the asset Tether (USDT) has been prominent.

8. The ability to utilise cryptocurrency as a money laundering tool is strengthened by USDT’s stable value (pegged to a dollar). Deals can be struck and payments made via other channels (bank transfers etc.) without volatility affecting the terms of the agreement.



Transaction Details

Transaction Hash: 0x042b7053bab1e80e5761adab3b223c3c576ff4e2a93c392d46cc5715308acefd

Status: ✓ Success

Block: 12290049 4 Block Confirmations

Timestamp: 53 secs ago (Apr-22-2021 12:38:28 PM +UTC) | Confirmed within 12 secs

From: 0xd7f8157fc629584c2b3c6f7291de1a373b045676

To: Contract 0x7a250d5630b4cf539739df2c5dacb4c659f2488d (Uniswap V2: Router 2) ✓
└ TRANSFER 0.11 Ether From Uniswap V2: Rout... To → Wrapped Et...

Transaction Action: Swap 0.11 Ether For 189,675,405.387924102848950964 SHIB On Uniswap

Tokens Transferred: 2
From Uniswap V2: Rout... **To** Uniswap V2: SHIB 4 **For** 0.11 ($284.71) Wrapped Ethe... (WETH)
From Uniswap V2: SHIB 4 **To** 0xd7f8157fc62958... **For** 189,675,405.387924102848950964 ($286.41) SHIBA INU (SHIB)

Value: 0.11 Ether ($284.20)

Transaction Fee: 0.0099856944 Ether ($25.80)

Gas Price: 0.0000001089 Ether (108.9 Gwei)

Click to see More ↓

Private Note: To access the Private Note feature, you must be Logged In

Demonstration

https://www.chainabuse.com/report/82855fa1-3851-4739-9fd8-f0af8b05ed6d?context=browse-chain&chain=ETH

- OSINT case: OXT graph visualiser / [https://www.ethtective.com /](https://www.ethtective.com/) mistrack.io
- TRM Forensics

Exercise 2

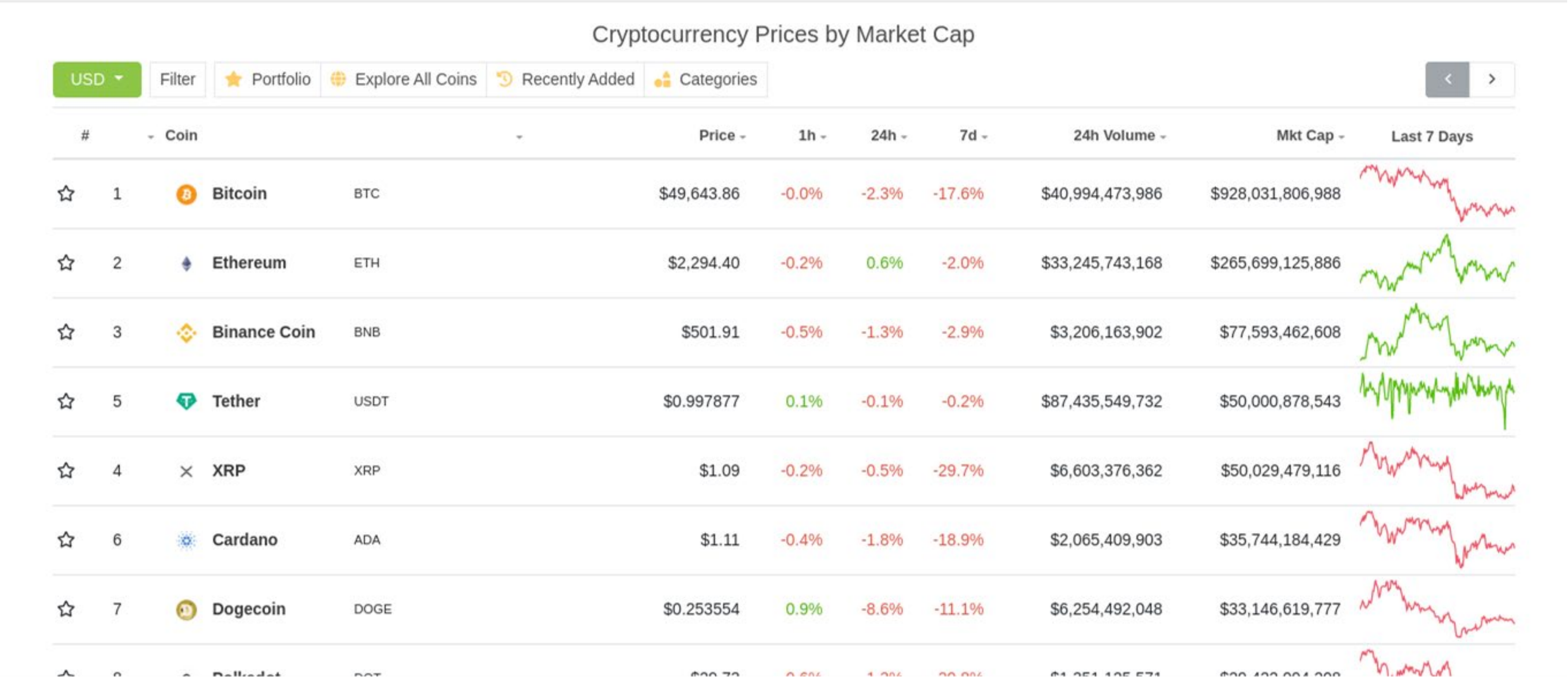
- Navigate to www.chainabuse.com/reports
- Click on Bitcoin
- Find an address detailed within a report and copy it
- Paste this into the following block explorers and review the transactions associated:
  - https://oxt.me
  - https://mempool.space/
  - www.blockchain.com

- Now do the same for Ethereum, return back to Chainabuse and click on Ethereum.
- Review the transactions linked to an address in the following block explorers:
  - https://debank.com/
  - https://etherscan.io/
  - https://eigenphi.io/

- Choose a Bitcoin and Ethereum transaction to show to the group (Highlight the TXID, the time/date, the inputs/outputs, the fee paid and any other detail you believe is relevant)

Exercise 2 cont.

- Login to TRM Forensics
- Start in block explorer and search for the relevant details
- Navigate to https://www.chainabuse.com/report/a36786da-b8d5-46df-b4a9-8f804fc63779?context=browse-chain&chain=BTC
- Break down the report and search for the relevant Bitcoin identifiers in Graph Visualiser. Corroborate the intelligence provided by the victim.
- Once completed outline an investigation strategy for progressing the matter. Include anything you think might be relevant to this.
- Have someone else present a briefing on what has happened, how the intelligence has been corroborated and what the onward investigation strategy is.



Cryptocurrency Prices by Market Cap

	#	Coin		Price	1h	24h	7d	24h Volume	Mkt Cap	Last 7 Days
☆	1	Bitcoin	BTC	$49,643.86	-0.0%	-2.3%	-17.6%	$40,994,473,986	$928,031,806,988	
☆	2	Ethereum	ETH	$2,294.40	-0.2%	0.6%	-2.0%	$33,245,743,168	$265,699,125,886	
☆	3	Binance Coin	BNB	$501.91	-0.5%	-1.3%	-2.9%	$3,206,163,902	$77,593,462,608	
☆	5	Tether	USDT	$0.997877	0.1%	-0.1%	-0.2%	$87,435,549,732	$50,000,878,543	
☆	4	XRP	XRP	$1.09	-0.2%	-0.5%	-29.7%	$6,603,376,362	$50,029,479,116	
☆	6	Cardano	ADA	$1.11	-0.4%	-1.8%	-18.9%	$2,065,409,903	$35,744,184,429	
☆	7	Dogecoin	DOGE	$0.253554	0.9%	-8.6%	-11.1%	$6,254,492,048	$33,146,619,777	
☆	8	Polkadot	DOT	$20.73	-0.6%	-1.2%	-20.8%	$1,251,125,571	$20,422,004,208	

What about the rest?

Monero: Key features

Ring CT:

Conceals the transaction amount

Ring Signatures:

Protect the sender by obfuscating which output was spent.

Dandalion++:

Obfuscates the transaction broadcast origin.

Stealth addresses:

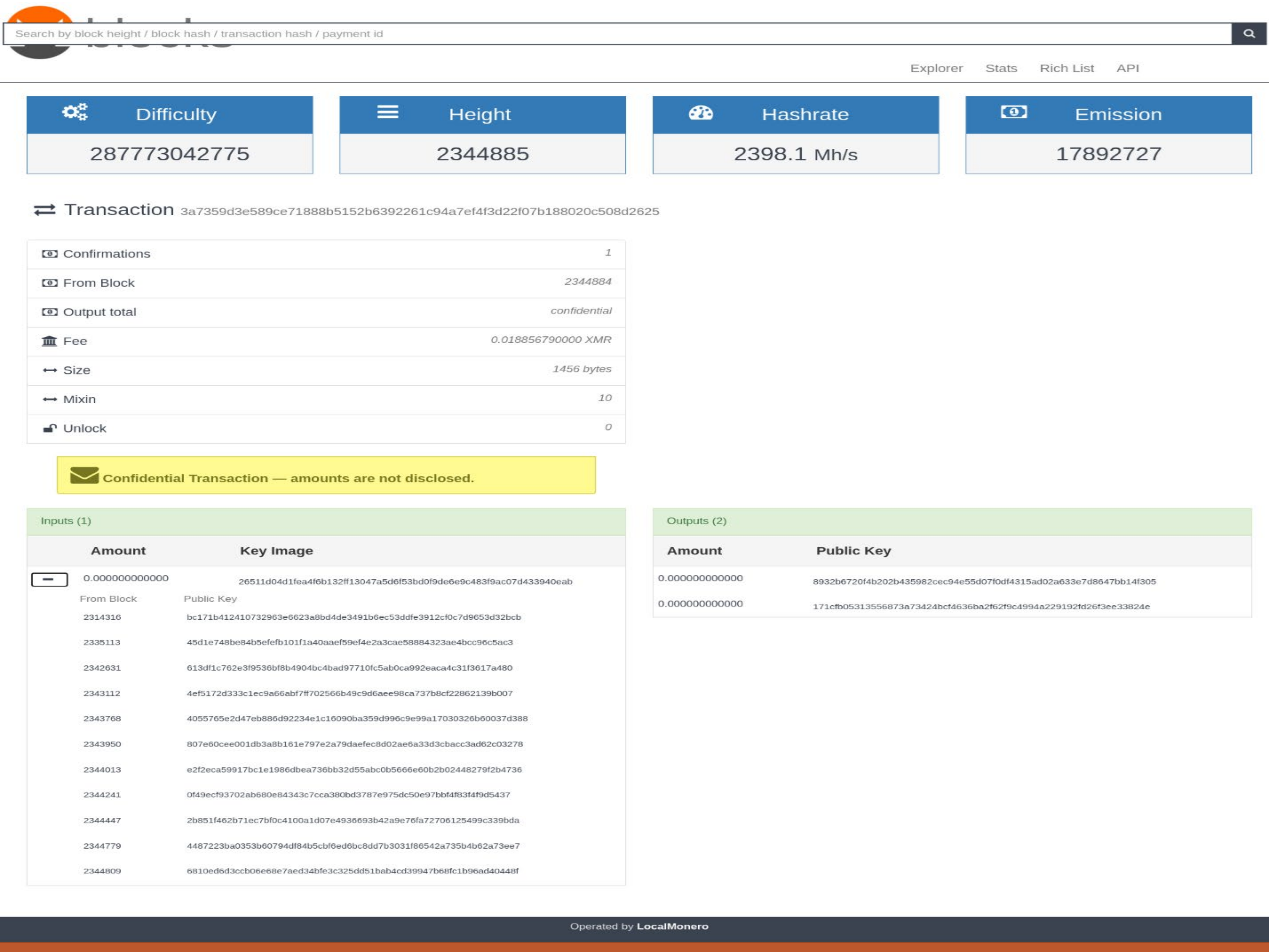
Ensure that the recipient's address is not recorded on the blockchain.

These features make tracing Monero very difficult. There are some options still available. These involve weakening the anonymity set, engagement with cryptocurrency services and timing analysis.

Monero is becoming a significant asset in ransomware attacks. Outside of this however it is still a long way behind Bitcoin. This is down to a smaller liquidity pool being available for the money laundering process

It is possible to swap from Monero into Bitcoin and this is likely the MO many would take to launder criminal proceeds.

This is not an easy process however as timing analysis can reveal the points at which the conversion takes place. It is then much easier to trace the Bitcoin assets as they move through the financial system.



Search by block height / block hash / transaction hash / payment id

Explorer Stats Rich List API

Difficulty	Height	Hashrate	Emission
287773042775	2344885	2398.1 Mh/s	17892727

⇄ Transaction 3a7359d3e589ce71888b5152b6392261c94a7ef4f3d22f07b188020c508d2625

Confirmations	*1*
From Block	*2344884*
Output total	*confidential*
Fee	*0.018856790000 XMR*
Size	*1456 bytes*
Mixin	*10*
Unlock	*0*

✉ **Confidential Transaction — amounts are not disclosed.**

Inputs (1)

Amount	Key Image
0.000000000000	26511d04d1fea4f6b132ff13047a5d6f53bd0f9de6e9c483f9ac07d433940eab

From Block	Public Key
2314316	bc171b412410732963e6623a8bd4de3491b6ec53ddfe3912cf0c7d9653d32bcb
2335113	45d1e748be84b5efefb101f1a40aaef59ef4e2a3cae58884323ae4bcc96c5ac3
2342631	613df1c762e3f9536bf8b4904bc4bad97710fc5ab0ca992eaca4c31f3617a480
2343112	4ef5172d333c1ec9a66abf7ff702566b49c9d6aee98ca737b8cf22862139b007
2343768	4055765e2d47eb886d92234e1c16090ba359d996c9e99a17030326b60037d388
2343950	807e60cee001db3a8b161e797e2a79daefec8d02ae6a33d3cbacc3ad62c03278
2344013	e2f2eca59917bc1e1986dbea736bb32d55abc0b5666e60b2b02448279f2b4736
2344241	0f49ecf93702ab680e84343c7cca380bd3787e975dc50e97bbf4f83f4f9d5437
2344447	2b851f462b71ec7bf0c4100a1d07e4936693b42a9e76fa72706125499c339bda
2344779	4487223ba0353b60794df84b5cbf6ed6bc8dd7b3031f86542a735b4b62a73ee7
2344809	6810ed6d3ccb06e68e7aed34bfe3c325dd51bab4cd39947b68fc1b96ad40448f

Outputs (2)

Amount	Public Key
0.000000000000	8932b6720f4b202b435982cec94e55d07f0df4315ad02a633e7d8647bb14f305
0.000000000000	171cfb05313556873a73424bcf4636ba2f62f9c4994a229192fd26f3ee33824e

Operated by **LocalMonero**

Exercise 3

- Return back to the investment fraud situation and implement the next aspect of your investigation strategy. If you need/want to choose a new report from Chainabuse, please make sure it is BTC related. Stop at the point you feel is appropriate and in line with the strategy devised.

- Create an audit trail of your actions and any relevant evidence using the case management system.

- Take note of anything you encounter which you don’t understand and want further input on.

- Prepare a briefing on your findings. Someone who has not presented to the group thus far will do so at the end of the time allotted.

The End!
Any questions?