
# Introduction to Virtual Assets

# High level overview

- **Natively digital** – Same as money transferred via traditional payment methods e.g. SWIFT.
- **Peer to peer** – Network sustained by participants, not a central third party.*
- **Blockchain** – The statement/ledger of all transactions
- **Addresses** – Used to transact, similar to account numbers
- **Wallets** – User controlled software which generates and stores addresses
- **Transaction identifiers** – Each transaction gets a unique identifier
- **Inputs and outputs** - Input are assets being spent and outputs are those created from the inputs.
- **Mining/Consensus** – The means of minting new coins and adding new transactions to the blockchain.
- **Transparent** – Many blockchains are easily auditable and so it is possible to attribute transaction activity to an address.
- **One or multiple** - Some cryptocurrencies use one address for all transactions activity, some use multiple.

# Consensus

- For Blockchain-based distributed systems:
  - enables a unified agreement
  - aligns economic or other incentives
  - insures fairness
  - enables fault-tolerance
  - ensures that everyone works on the same state of the world
- Proof of Work; Expending costly resources
- Proof of Stake; Commitment of value
- Consortium: Set number of known/validated verifiers
- This is an evolving subject so don’t get too hung up on this aspect

# 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** | |

# Use cases

- Digital cash
- Store of value
- Financial markets
- Music
- Digital ownership
- Communication
- Identity
- Governance/legal
- Gaming
- Storage
- Supply chains
- Hospitality
- Energy
- Health

# Difficulties

- Challenge for law enforcement is that criminality will exploit the various use cases.
- An example is the energy sector. Increased focus on green energy and recycling has opened up numerous avenues for money laundering.
- There is too much for active investigators to manage in relation to this subject.
- Effective strategies need to be implemented throughout the relevant LEA. These need to consider resources, training, horizon scanning and remits.
- Getting buy in from senior management is vital.

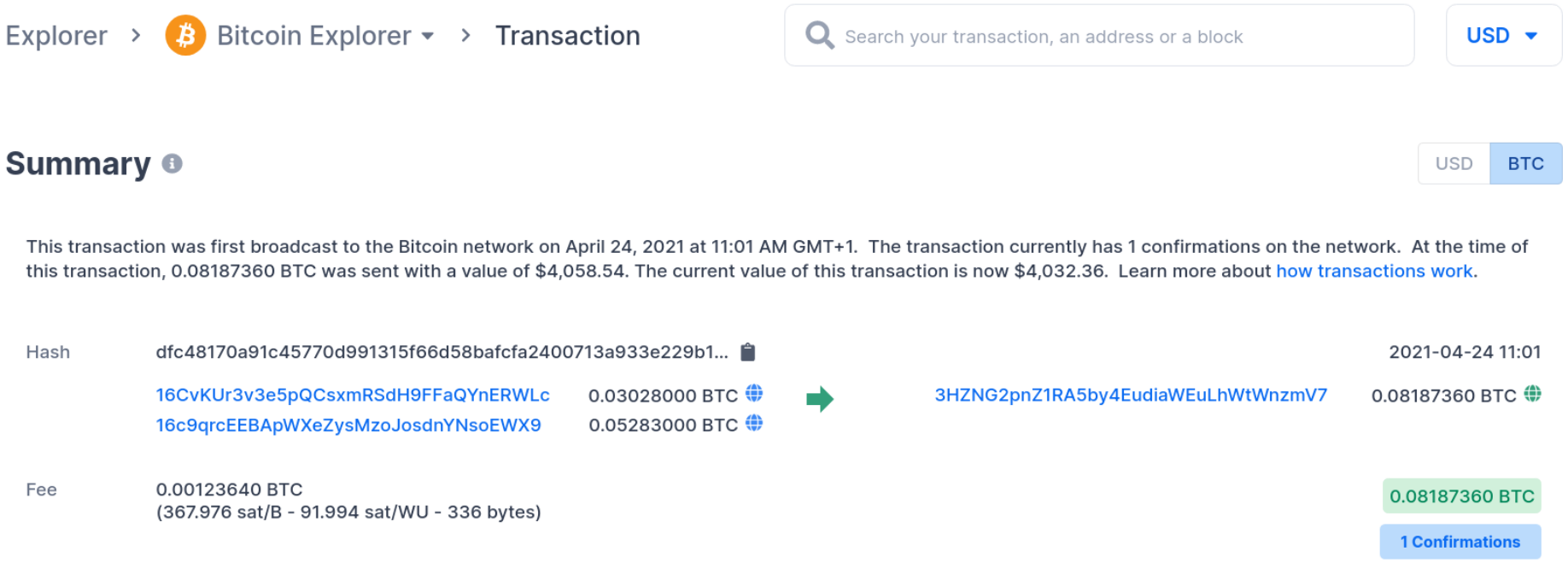
# Practical 1

| | |
|---|---|
| Wallet | Install Bluewallet from Google Play or the Apple App Store |
| Mnemonic | Click on “Add Wallet” and select “Bitcoin”. The mnemonic representing the “private key” is now displayed. This needs to be written down. Once done click on “Ok I wrote it down” |
| Receiving | Click on the blue box titled “Wallet” which displays “0 BTC”. Now select “Receive” and click “Yes I have”. |
| Address | The QR code is a representation of the address (account number) and underneath the address is written out (alpha numeric starting “bc1q”) |
| HD wallet | Click back and then select the options/settings menu within the wallet. Click on Show addresses, review both “Receive” and “Change” headings.<br>Explore the options within the app. Try turning on “Advanced mode” in settings (come out to the main screen and it’s under “General”). Create a new wallet and select “Segwit, what is different about the address? |
| Questions | Consider this process and confer in your breakout groups on what questions it raises. Choose the most poignant one for sharing with the rest of the participants |

# Practical 2 (See video)

**Using Bluewallet on a mobile device**

- **Click “Add wallet”**
- **Select “Lightning” and click “Create”**
- **Copy (by clicking on) the text starting “lndhub://” and paste this into a notes application.**
- **Then click “Ok I’ve saved it”**
- **On the displayed screen select the Yellow background displaying “Wallet” and “0 Sats”.**
- **Select “Receive” and then click on “Scan”.**
- **Point your camera at the QR code on the right and once recognized you will see a page titled “Receive” and an amount displayed of 50 sats. Click on “Create Invoice”**
- **Choose “Ok” for notifications**
- **Congratulations you now have 0.0000005 Bitcoin! Let’s try out spending.**
- **Navigate in a browser to https://paywall.link/to/e4968**
- **Now in your Lightning wallet select “Send” and then click “Scan”.**
- **Confirm the payment and…Voilà! You have access to the resource.**




# Anatomy of a Bitcoin transaction

## Inputs

HEX ASM

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

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

## Outputs

| | | | |
|---|---|---|---|
| Index | 0 | Details | Unspent |
| Address | 3HZNG2pnZ1RA5by4EudiaWEuLhWtWnzmV7 | Value | 0.08187360 BTC |
| Pkscript | OP_HASH160<br>ae0fa915f65c6fe4ebaa19d29237368fb43a66af<br>OP_EQUAL | | |

Cryptocurrency Prices by Market Cap

USD | Filter | Portfolio | Explore All Coins | Recently Added | Categories

| # | 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 |  |

# What about the rest?

# 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). This allows for deals to be struck and payments made via other channels (bank transfers etc.) without volatility affecting the terms of the agreement.

# Transaction Details

Buy Exchange Earn Gaming

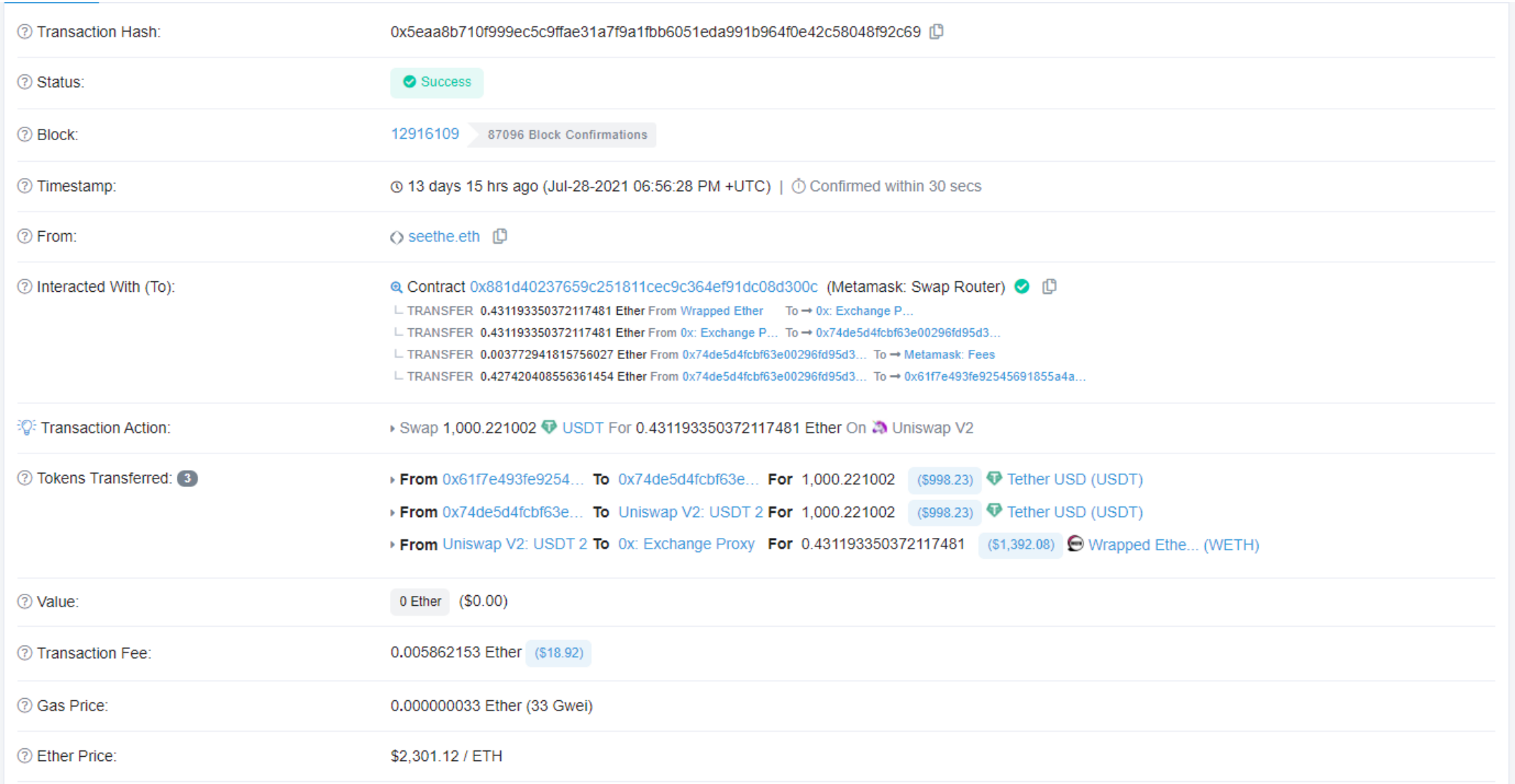
Overview | Internal Txns | Logs (5) | State | Comments

| | |
|---|---|
| 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)<br>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)<br>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 |

- DeFi does confuse things a bit!



| | |
|---|---|
| Transaction Hash: | 0x5eaa8b710f999ec5c9ffae31a7f9a1fbb6051eda991b964f0e42c58048f92c69 |
| Status: | Success |
| Block: | 12916109 87096 Block Confirmations |
| Timestamp: | 13 days 15 hrs ago (Jul-28-2021 06:56:28 PM +UTC) \| Confirmed within 30 secs |
| From: | seethe.eth |
| Interacted With (To): | Contract 0x881d40237659c251811cec9c364ef91dc08d300c (Metamask: Swap Router)<br>TRANSFER 0.431193350372117481 Ether From Wrapped Ether To 0x: Exchange P...<br>TRANSFER 0.431193350372117481 Ether From 0x: Exchange P... To 0x74de5d4fcbf63e00296fd95d3...<br>TRANSFER 0.003772941815756027 Ether From 0x74de5d4fcbf63e00296fd95d3... To Metamask: Fees<br>TRANSFER 0.427420408556361454 Ether From 0x74de5d4fcbf63e00296fd95d3... To 0x61f7e493fe92545691855a4a... |
| Transaction Action: | Swap 1,000.221002 USDT For 0.431193350372117481 Ether On Uniswap V2 |
| Tokens Transferred: 3 | From 0x61f7e493fe9254... To 0x74de5d4fcbf63e... For 1,000.221002 ($998.23) Tether USD (USDT)<br>From 0x74de5d4fcbf63e... To Uniswap V2: USDT 2 For 1,000.221002 ($998.23) Tether USD (USDT)<br>From Uniswap V2: USDT 2 To 0x: Exchange Proxy For 0.431193350372117481 ($1,392.08) Wrapped Ethe... (WETH) |
| Value: | 0 Ether ($0.00) |
| Transaction Fee: | 0.005862153 Ether ($18.92) |
| Gas Price: | 0.000000033 Ether (33 Gwei) |
| Ether Price: | $2,301.12 / ETH |

Interpretation: Sender uses smart contract to move from USDT to WETH, this is potentially held on a DeFi platform providing liquidity. The sender would potentially be earning yield on this.

# 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.**

| 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 |

Quiz time!
https://forms.gle/xPRLXQUgnZBL4X55A

**The End!**
**Any questions?**