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

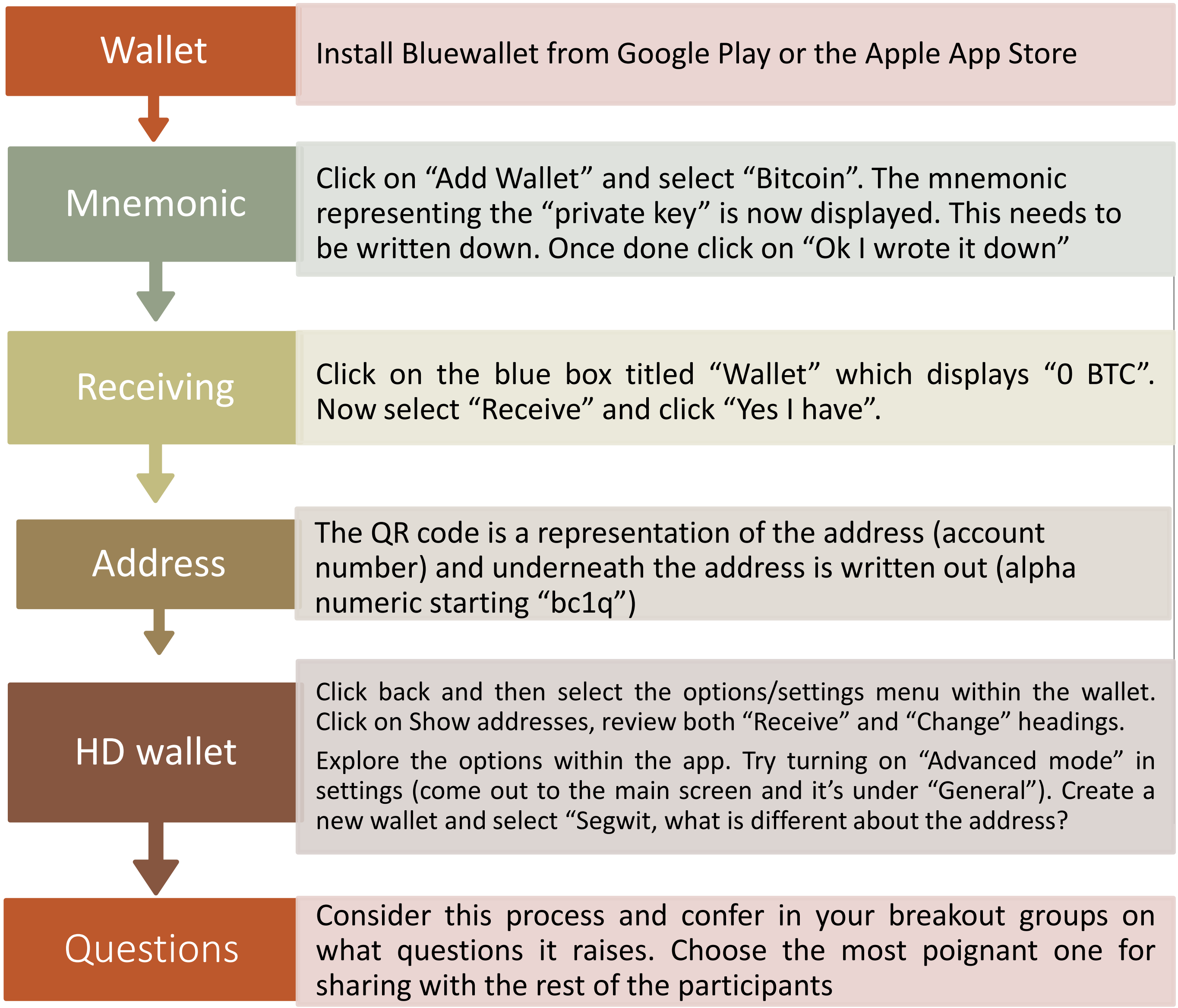
Jargon: There is a lot of this!

- 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

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”)

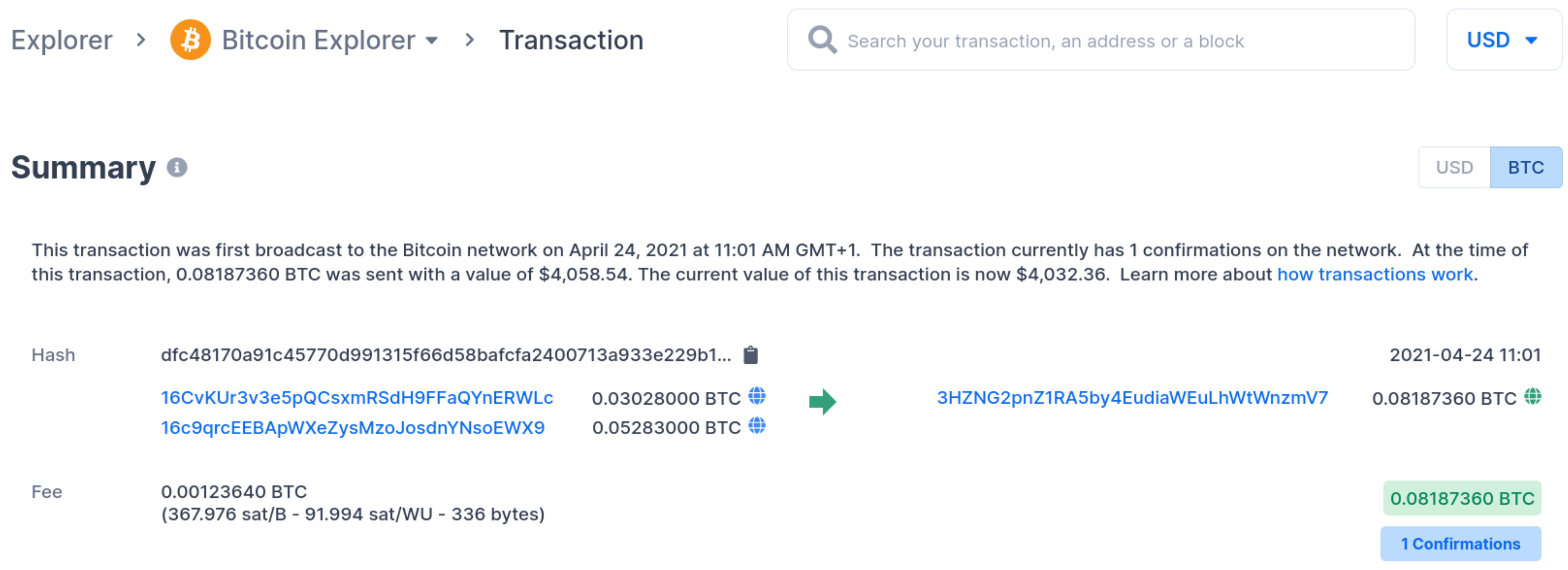
HD wallet

Click back and then select the options/settings menu within the wallet. Click on Show addresses, review both “Receive” and “Change” headings.

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



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

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

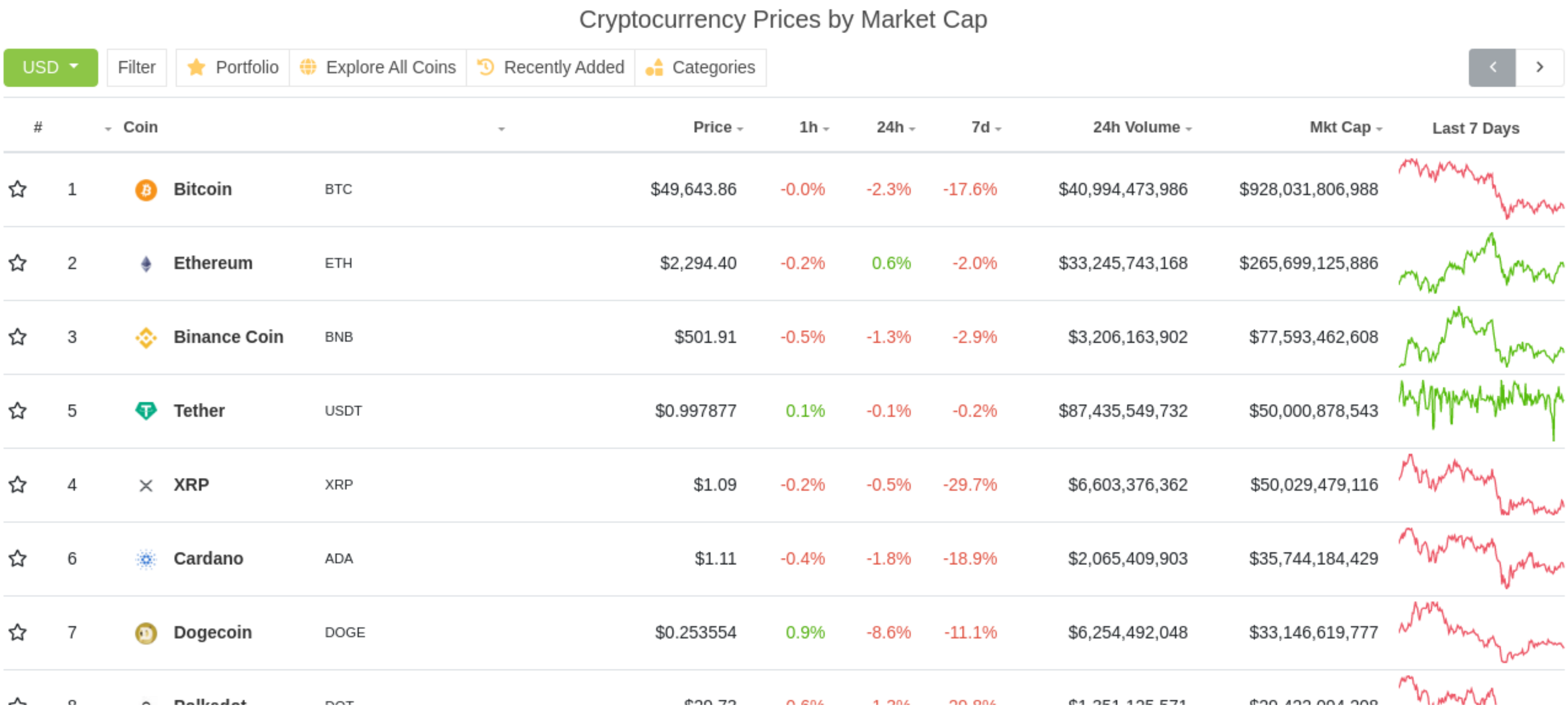
16CvKUr3v3e5pQCsxmRSdH9FFaQYnERWLc 0.03028000 BTC
16c9qrcEEBApWXeZysMzoJosdnYNsoEWX9 0.05283000 BTC
→ 3HZNG2pnZ1RA5by4EudiaWEuLhWtWnzmV7 0.08187360 BTC

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

0.08187360 BTC

1 Confirmations

Anatomy of a Bitcoin transaction



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	$29.73	-0.6%	-1.3%	-29.8%	$1,251,125,571	$29,422,094,208	

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.

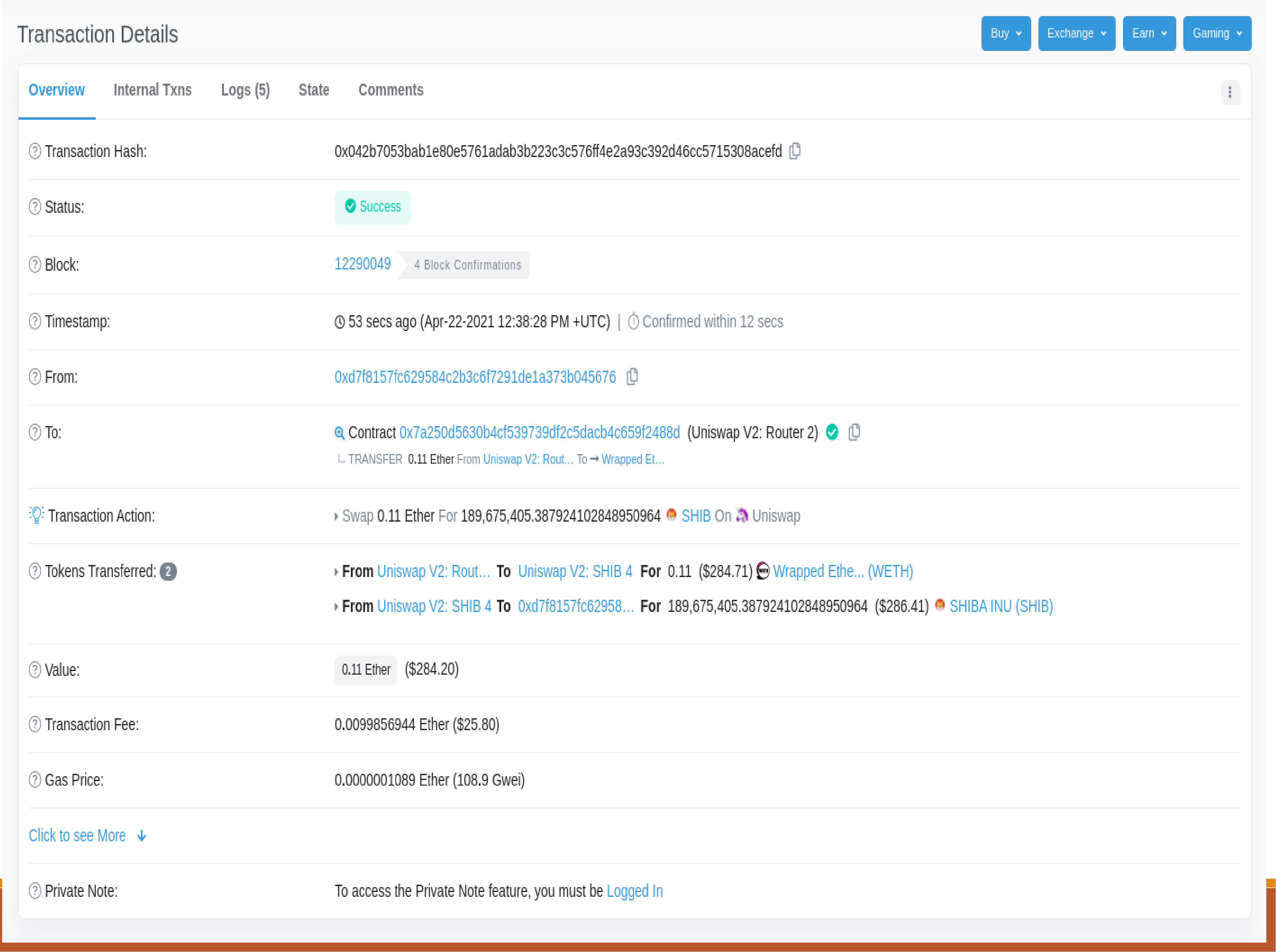
4. It is possible to utilise the transparent nature of many smart contracts to follow the route an asset has taken.

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

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

Money Laundering

- Professional money laundering facilitators/controllers/networks are increasingly taken advantage of cryptocurrencies.
- They will use whatever cryptocurrency/virtual asset protocol that suits their purpose. An example is the transition to protocols with lower fees (ETH to TRON).
- Stablecoins in particular are attractive to these networks. They remove the volatility aspect of floating assets whilst still enabling fast international payments which do not touch traditional financial networks. This make negotiations and conversions to cash values much easier to navigate.
- Importantly cryptocurrencies are not becoming the asset desired as the end product. Clean cash or bank transfers are still the most desirable financial mechanisms. As such cryptocurrencies have just become another weapon in the money laundering arsenal.

Money laundering cont.

- One particular tactic identified in a number of instances has been the formation of digital payment companies. These are incorporated are seen as a vehicle to facilitate OTC accounts with mainstream, highly liquid cryptocurrency exchanges. Money laundering activity is then hidden as trading activity with professional enablers assisting in falsifying AML/KYC checks.
- It has also become very apparent that organised crime groups are seeking out entities who can facilitate money laundering involving cryptocurrencies. As a result, professional networks are servicing multiple OCG's within one or more jurisdictions. International corruption cases are also seeing these networks as key aspects of money laundering processes.
- The same tactics are still used e.g. IVTS, using willing/unwilling money mules on an international scale, multiple types of accounts across many financial services, high volumes of intermediary transactions, moving from one currency to another, using shell/front companies, and combining multiple crime types e.g. MTIC fraud with traditional crime types with money laundering as a service.

Money laundering cont.

Cryptocurrency protocols/network do offer some unique opportunities for money laundering:

Non-Fungible Tokens (NFT's) – These tokens are cryptographic proof of ownership for real world or digital items. They act in a similar fashion as bearer bonds; control of the private key is defacto proof of ownership. The current focus for NFT's is art and gaming items. Recent sales at auction houses such Sotheby's have seen NFT's go for millions of dollars. Beyond the current focus there is a drive to increase the adoption of NFT's across a broad spectrum of industries e.g. act as festival tickets, proof of identity, access to platform, etc.

With a liquid market for such items and many tools to facilitate such activity it would seem a matter of time before criminal exploitation is a factor. An example of this could be money laundering entities arranging a series of consecutive sales and purchases for an NFT. This can also be used to manipulate the price of NFT's.

Cryptocurrency specific shell/front entities - DeFi projects have used alternative funding models to bypass the controversial ICO structures of 2017 (e.g. entities must provide a service to the project in reward for tokens). This has, to date, allowed these projects to skirt regulation and scrutiny. It is already suspected that sophisticated criminal actors have utilised DeFi to launch projects which have rigged the issuance of tokens and taken in significant amounts of criminal proceeds.

Such vehicles for money laundering offer several advantages, for example the entities behind the project can use aliases/pseudonyms as in the project will not have a business entity registered. This is because a smart contract will be used to control the platform and the term "decentralised" will be used to claim it is not run by any one entity, but the community holding "governance" tokens.

Private sector input

"*Fraud is the dominant cryptocurrency crime*": Fake investment platforms, romance fraud, compromising accounts, exit scams, corruption.

Compromise of DeFi smart contracts is the most significant contributor to financial losses. The money laundering which takes place after this involves moving between different assets through DEX's and attempting to chain swap where possible. This is why reporting on the matter has highlighted the rise in illicit finances being moved through DEX protocols.

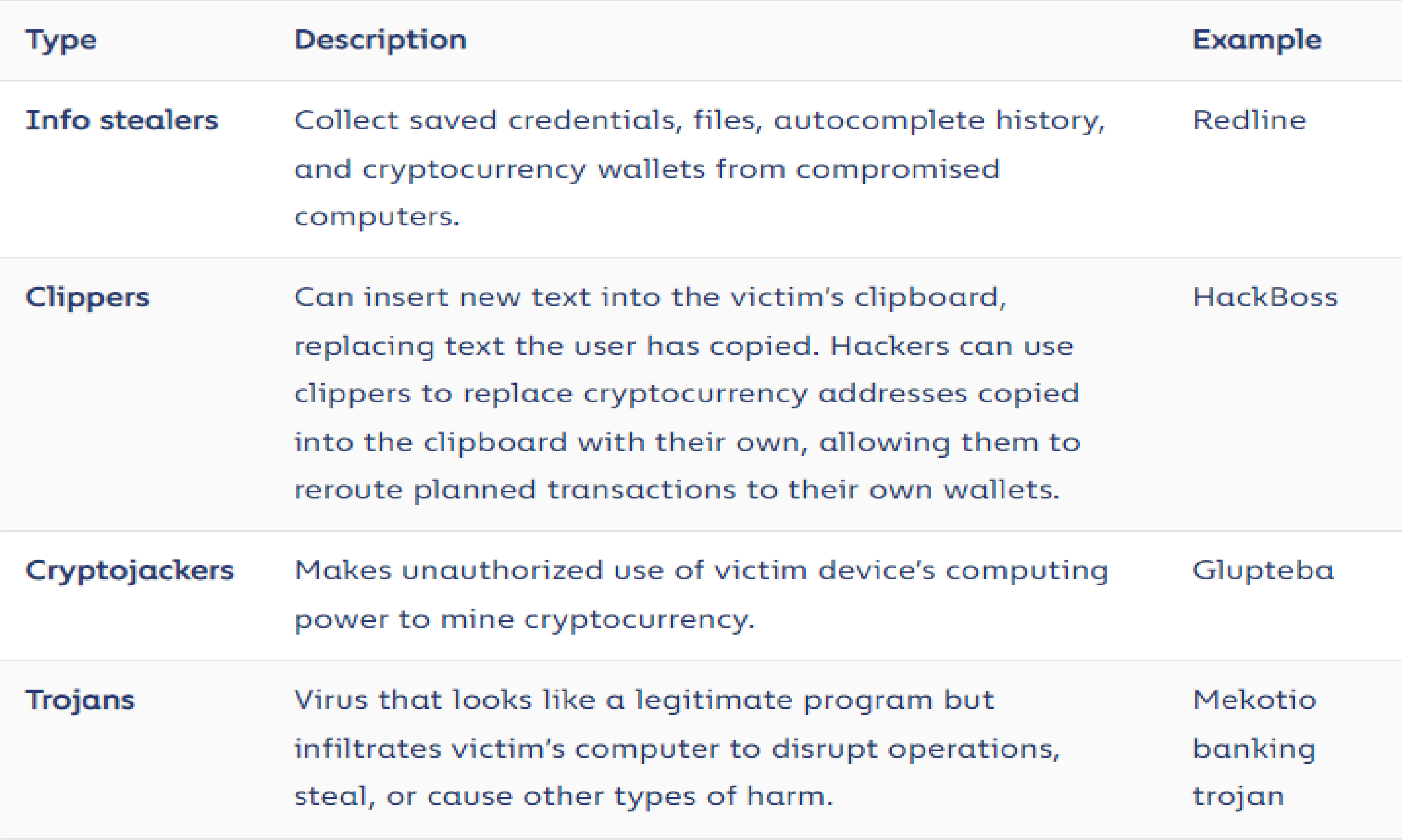
The transparency of most platforms and the centralisation of many projects has led to offenders having significant issues in laundering funds. There have even been instances where the offender has returned all the funds after negotiating a "finders fee"!

Corporate investigation entities are also reporting that a rising number of instances involving cryptocurrency assets.

Terrorist financing is still largely based in legacy financial systems however there have been more instances of reports highlighting the use of cryptocurrency:

"In addition to bitcoin and Ethereum, the seizure order demonstrates that Hamas also collected donations in Tether, TRON, Cardano, XRP, and DOGE, indicating their attempts to break out from reliance on bitcoin after the US DoJ announced the seizure of $2 million in cryptocurrency from prominent terrorist groups."

Cryptocurrency focused malware



Type	Description	Example
Info stealers	Collect saved credentials, files, autocomplete history, and cryptocurrency wallets from compromised computers.	Redline
Clippers	Can insert new text into the victim's clipboard, replacing text the user has copied. Hackers can use clippers to replace cryptocurrency addresses copied into the clipboard with their own, allowing them to reroute planned transactions to their own wallets.	HackBoss
Cryptojackers	Makes unauthorized use of victim device's computing power to mine cryptocurrency.	Glupteba
Trojans	Virus that looks like a legitimate program but infiltrates victim's computer to disrupt operations, steal, or cause other types of harm.	Mekotio banking trojan

Courtesy of Chainalysis research

Difficulties

- Challenge for law enforcement is that criminality will dynamically 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.
- To achieve this getting buy in from senior management is vital.

The End!

Any questions?

Blockchain analysis

Heuristics

- **“Clustering addresses”** refers to the process of attributing numerous addresses to the same wallet/controlling entity through the use of transaction behaviour heuristics.

- There are a number of factors which go into these heuristics. We will cover some of the well known ones in the following slide. It is important to note however that none of the heuristics are definite. They can be wrong and as investigators it is necessary to corroborate the results.

- Cryptocurrencies focused on principles of self sovereignty recognise blockchain analysis as an attack on the network. **Small minorities within these communities are working to break the heuristics used and minimise the ability to undermine privacy within the protocol.**

- The key point here is that the methods being used to provide Blockchain Forensic Tools is likely to evolve in line with efforts to break the heuristics. It could become more difficult to identify how results are being provided and this makes it important to keep informed on the subject.

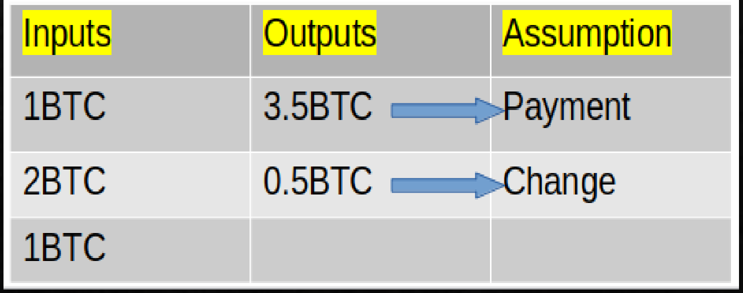
Heuristic 1 – Common Input Ownership

Assumption: All inputs in a transaction belong to the same entity as they reside in the same wallet.

- ❑ Vast majority of bitcoin transactions are simple in nature. Very few collaborative transactions.
- ❑ As a result one wallet controlled by one entity will have provided all of the transaction inputs to send funds.

Heuristic 2 – Change address detection:

- Change amounts are linked to addresses never previously seen in the blockchain.
- If an output address is the same as an input address it is the change.
- Wallet fingerprinting can be used to detect change outputs because a change output is the one spent with the same wallet fingerprint.
- Round numbers as an output are payments not change.
- If the values of the inputs are more than one of the outputs but less than another, the lower figure output is change (Unnecessary input heuristic) e.g.



Inputs	Outputs	Assumption
1BTC	3.5BTC →	Payment
2BTC	0.5BTC →	Change
1BTC		

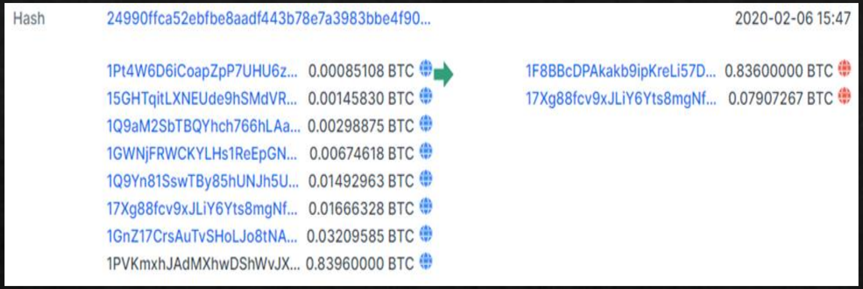
Assumptions:

- **If an output address has been reused it is very likely to be a payment output**, not a change output. This is because change addresses are created automatically by wallet software but payment addresses are manually sent between humans.

- Entities utilise wallet defaults for coin selection and fee payments.

- **Many payment amounts are round numbers**, for example 1 BTC or 0.1 BTC. The leftover change amount would then be a non-round number (e.g. 1.78213974 BTC). This potentially useful for finding the change address. The amount may be a round number in another currency. The amount 2.24159873 BTC isn't round in bitcoin but when converted to USD it may be close to an exact dollar value.

Heuristic examples

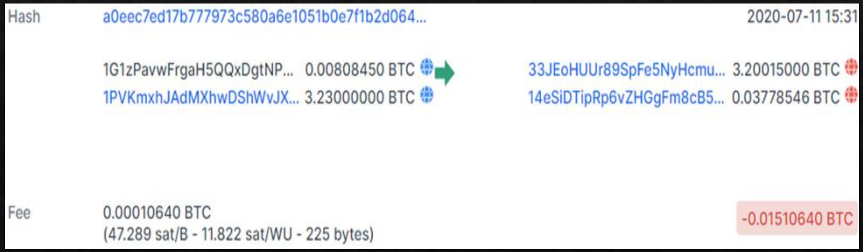


```
Hash    24990ffca52ebfbe8aadf443b78e7a3983bbe4f90...                                  2020-02-06 15:47

        1Pt4W6D6iCoapZpP7UHU6z...   0.00085108 BTC  →   1F8BBcDPAkakb9ipKreLi57D...  0.83600000 BTC
        15GHTqitLXNEUde9hSMdVR...   0.00145830 BTC      17Xg88fcv9xJLiY6Yts8mgNf...  0.07907267 BTC
        1Q9aM2SbTBQYhch766hLAa...   0.00298875 BTC
        1GWNjFRWCKYLHs1ReEpGN...    0.00674618 BTC
        1Q9Yn81SswTBy85hUNJh5U...   0.01492963 BTC
        17Xg88fcv9xJLiY6Yts8mgNf... 0.01666328 BTC
        1GnZ17CrsAuTvSHoLJo8tNA...  0.03209585 BTC
        1PVKmxhJAdMXhwDShWvJX...    0.83960000 BTC
```

Common input heuristic

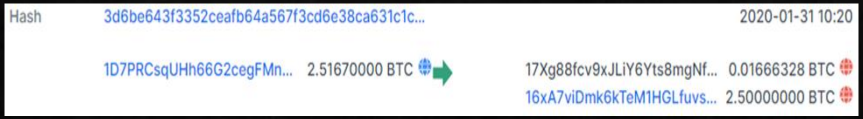
Change heuristic: Outputs are different script types.



```
Hash    a0eec7ed17b777973c580a6e1051b0e7f1b2d064...                                    2020-07-11 15:31

        1G1zPavwFrgaH5QQxDgtNP...   0.00808450 BTC  →   33JEoHUUr89SpFe5NyHcmu...   3.20015000 BTC
        1PVKmxhJAdMXhwDShWvJX...    3.23000000 BTC      14eSiDTipRp6vZHGgFm8cB5...  0.03778546 BTC


Fee     0.00010640 BTC                                                              -0.01510640 BTC
        (47.289 sat/B - 11.822 sat/WU - 225 bytes)
```



```
Hash    3d6be643f3352ceafb64a567f3cd6e38ca631c1c...                                   2020-01-31 10:20

        1D7PRCsqUHh66G2cegFMn...    2.51670000 BTC  →   17Xg88fcv9xJLiY6Yts8mgNf...  0.01666328 BTC
                                                        16xA7viDmk6kTeM1HGLfuvs...   2.50000000 BTC
```

Change heuristic: The address 16xA7 was active prior to this transaction. The address 17Xg88 was first active as part of this transaction. Round payment made to 16xA7 address

Private intelligence

Further to these heuristics Blockchain Forensic Tools will **utilise industry intelligence and covert surveillance tactics to attribute entities to addresses and build clusters**. This will mean it is often **opaque as to how an identification or cluster has been developed.**

It is possible to try and find connections. You can manually check for the heuristics and carry out open source research. This may however become unpractical (if significant amounts of data) or turn out to be inconclusive. In these instances it would be worth noting down the efforts made and the negative result. Such process will at least show efforts have been made to understand the intelligence and quantify it’s origins.

Practical example

- https://www.reddit.com/r/Electrum/comments/a9x374/my_electrum_just_got_hacked/
- Chain swapping example