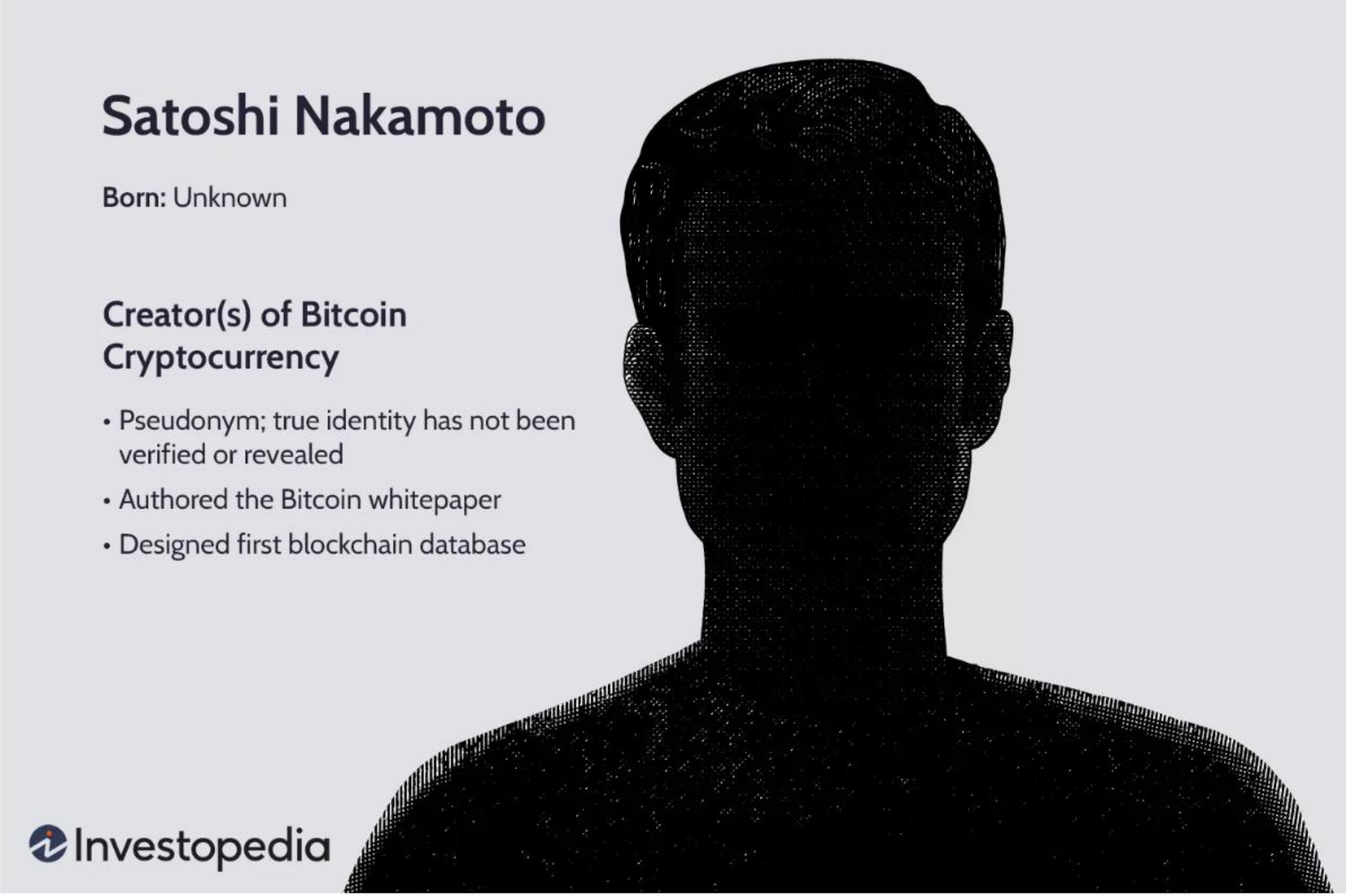
CRYPTOASSET BASICS

Or who is Satoshi Nakamoto?



Satoshi Nakamoto

Born: Unknown

Creator(s) of Bitcoin Cryptocurrency

- Pseudonym; true identity has not been verified or revealed
- Authored the Bitcoin whitepaper
- Designed first blockchain database

Investopedia / Bailey Mariner

WHERE DID IT ALL BEGIN?

- Satoshi Nakamoto is an alias for the person (or people) who developed the first Bitcoin software in 2008
- He/They remained active in Bitcoin and blockchain development until 2010 when he/they disappeared
- Not the first to float the concept of cryptocurrency but he solved the one major problem – “double-spending”
- How? – creation of the Blockchain system of verification
- He penned the original whitepaper on Bitcoin
- Several people over the years have claimed to be him but have never been verified
- Several people though to be him – never revealed
- Whoever it is they are a Billionaire as rumoured to hold circa 1 Million Bitcoin

22ND MAY 2010

Anyone know why this date is famous?

BITCOIN PIZZA DAY

Laszlo Hanyecz paid 10,000 BTC for two large pizzas

He posted on a Bitcoin forum "I'll pay 10,000 Bitcoins for a couple of pizzas. Like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later"

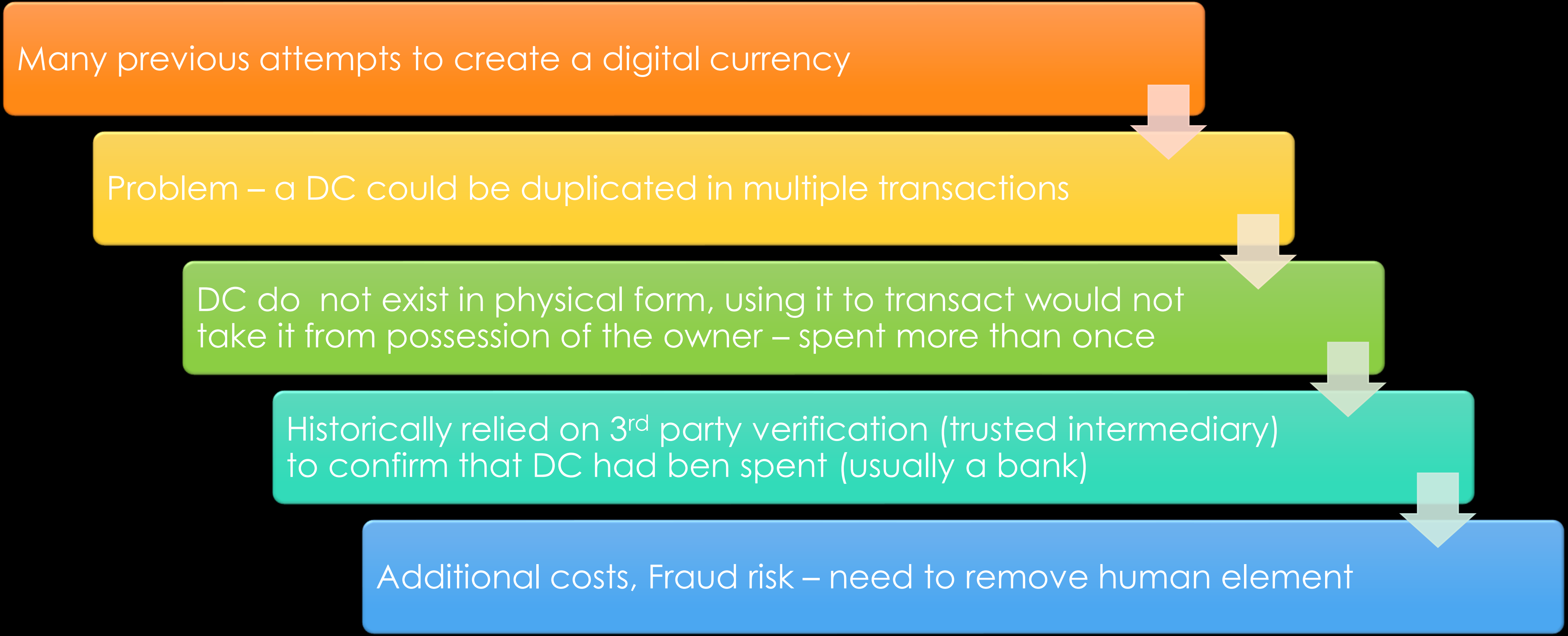
He reported a few days later that he had successfully made the trade

Value then $40. Value 2022 - $300M

This is believed to be the first real world transaction using Bitcoins

Bitcoin officially started trading in July 2010 – end of year worth $0.80.

BITCOIN:A PEER-TO-PEER ELECTRONIC CASH SYSTEM



Many previous attempts to create a digital currency

Problem – a DC could be duplicated in multiple transactions

DC do not exist in physical form, using it to transact would not take it from possession of the owner – spent more than once

Historically relied on 3rd party verification (trusted intermediary) to confirm that DC had ben spent (usually a bank)

Additional costs, Fraud risk – need to remove human element

THE SOLUTION?

Cryptography via an automated group consensus mechanism

Nakamoto proposed a Decentralised approach utilising multiple techniques

Timestamps added to each transaction

Cryptographic techniques used to encrypt data

The encrypted data cannot be amended or altered – can only be verified

The network verifies the transactions – majority consensus mechanism – Proof of Work

WHAT IS A BLOCKCHAIN?

It is a digitally distributed shared ledger which is publicly available to all

It exists across a network of computers so that the records cannot be altered historically and new blocks can only be added by consensus of the network

It can be used for a variety of purposes but the main ones being to record transactions and track the usage, or ownership of assets

Blockchain technology first drafted in 1991 as a way of recording timestamps which could not be altered

In the late 90s Nick Szabo proposed using one to secure a digital payments system – bit gold – never created

4 different types – Public Blockchain, Private Blockchain, Hybrid Blockchain, Consortium Blockchain

At least 1,000 different blockchains in existence – September 2022

DISTRIBUTED LEDGER TECHNOLOGY

It is the technological infrastructure and protocols which allow simultaneous access, validation and record updating across a network of multiple entities

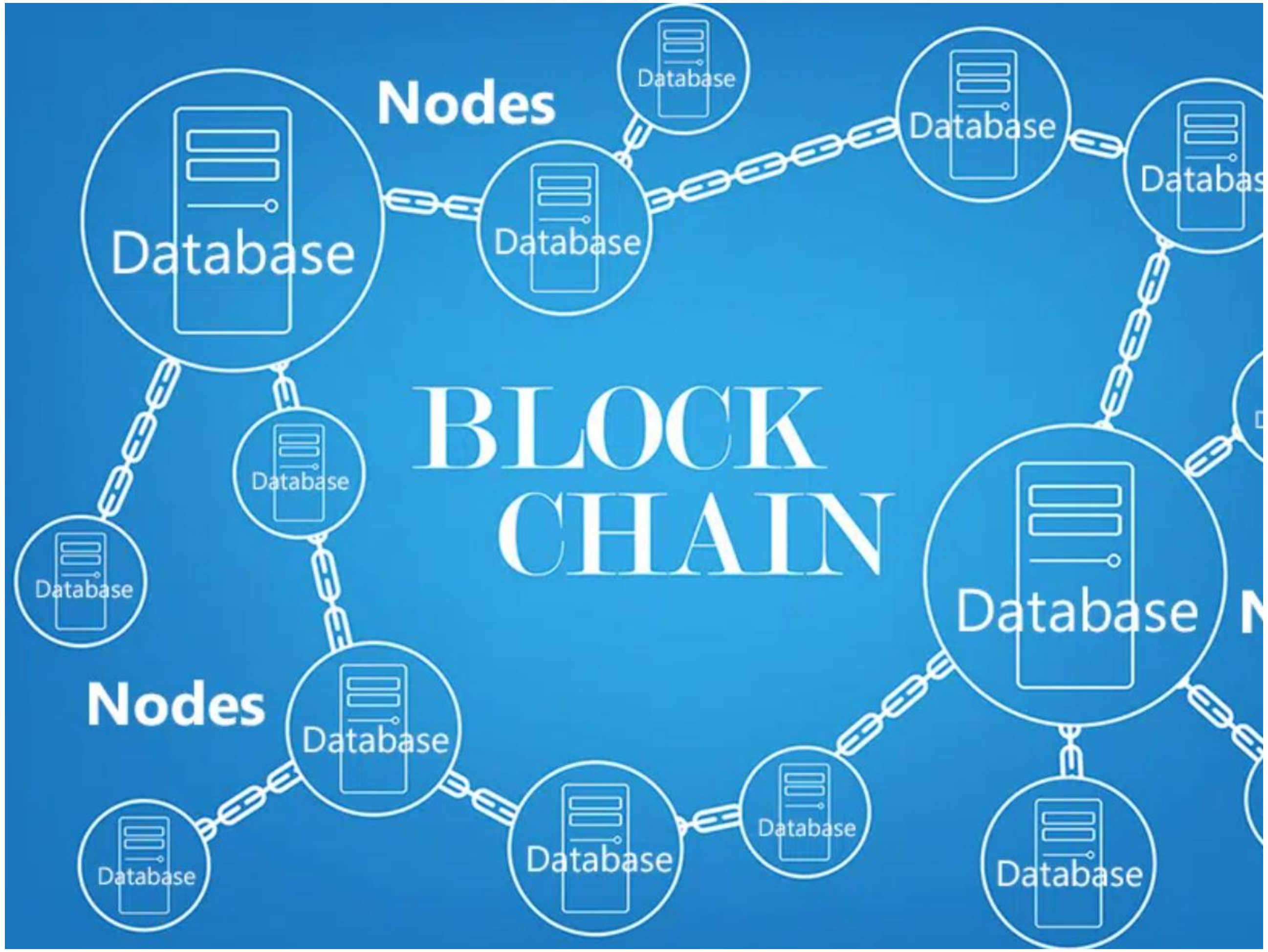
It is decentralised digital database using cryptography to secure and record the data accurately

Contains records of every transaction ever conducted in chronological order.

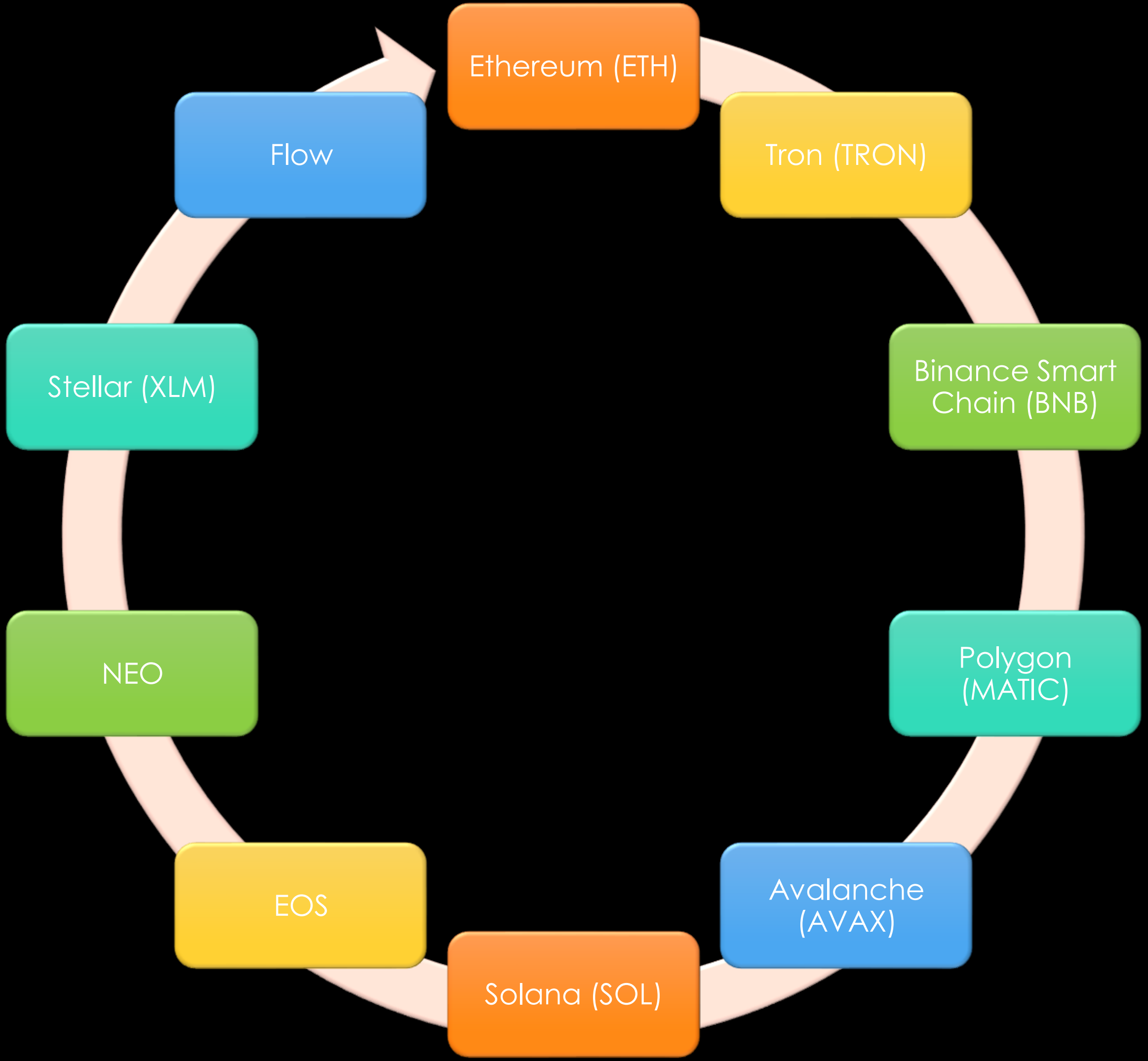
Distributed means it is public platform not owned or controlled by any one person or institution or even a group of people

DLT & BLOCKCHAIN

- Each client computer of the network is a Node and they form the decentralised network between them
- Update to the blockchain each node updates the DL and ensure there is consensus across all nodes as to true form of ledger
- When majority of nodes agree on the true form this is called Consensus



TOP 10 BLOCKCHAINS



Ethereum (ETH)

Tron (TRON)

Binance Smart Chain (BNB)

Polygon (MATIC)

Avalanche (AVAX)

Solana (SOL)

EOS

NEO

Stellar (XLM)

Flow

BLOCKCHAIN TERMINOLOGY

Total Value Locked – values of all assets staked in a DeFi platform's smart contracts for borrowing and lending capabilities – (TVL)

Transactions Per Second – maximum number of transactions a blockchain network can proves in a single second – (TPS) also known as Throughput Rate

Protocol – these are the fundamental rules which define how the blockchain platform is structured

Consensus Mechanism – the method by which the blockchain peers come to an agreement on the current status of the data

Ethereum – TVL $30.23B TPS 25 Protocols 25 Consensus – PoS

Tron – TVL $5.32B TPS 2,000 2,000 Protocols 2,000 Consensus – Delegated PoS

BNB – TVL $5.22B TPS 45 Protocols 469 Consensus - PoS Authority

Polygon – TVL $1.29B TPS 7,000 Protocols 309 Consensus – PoS

Avalanche – TVL $1.6B TPS 5,000 Protocols 255 Consensus – PoS

Solana – TVL $1.28B TPS 29,000 Protocols 81 Consensus – PoS and PoH (History)

EOS – TVL $110.27M TPS 4,000 Protocols 22 Consensus – Delegated PoS

NEO – TVL $38.2M TPS 1,000 Protocols 3 Consensus – Federated Byzantine Agreement (FBA)

Stellar – TVL $23.25M TPS 1,000 Protocols 3 Consensus – FBA

Flow – TVL $3.68M TPS 10,000 Protocols 2 Consensus - PoS

WHAT IS PROOF OF WORK?

Decentralised consensus mechanism requiring members of a network to race to solve a mathematical puzzle

Used in mining for the validation of transactions and the mining of new tokens

It allows Bitcoin transactions to be processed securely without need for 3rd party validation

It requires massive amount of energy, which increased as more miners join in and try and solve the puzzle

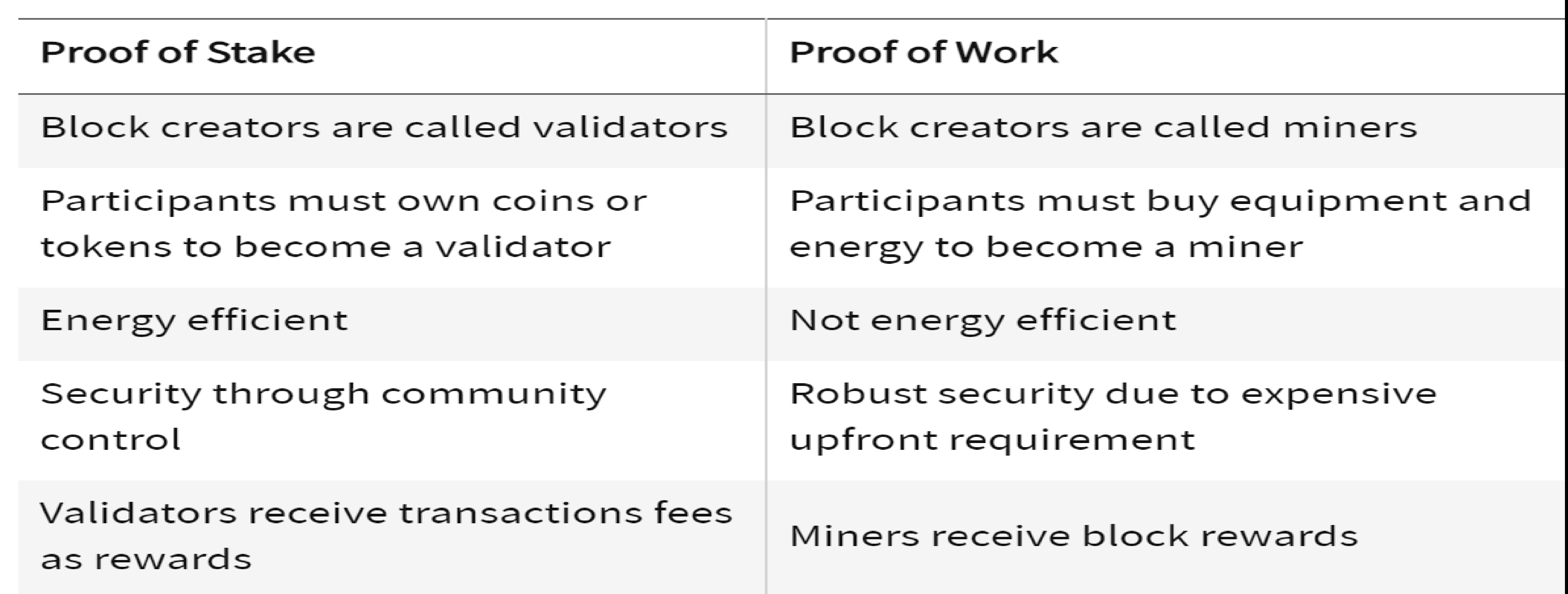
Used concept developed by Hal Finney in 2004 "reusable proof of work"

Finney was supposedly the recipient of the first Bitcoin transaction

WHAT IS PROOF OF STAKE?

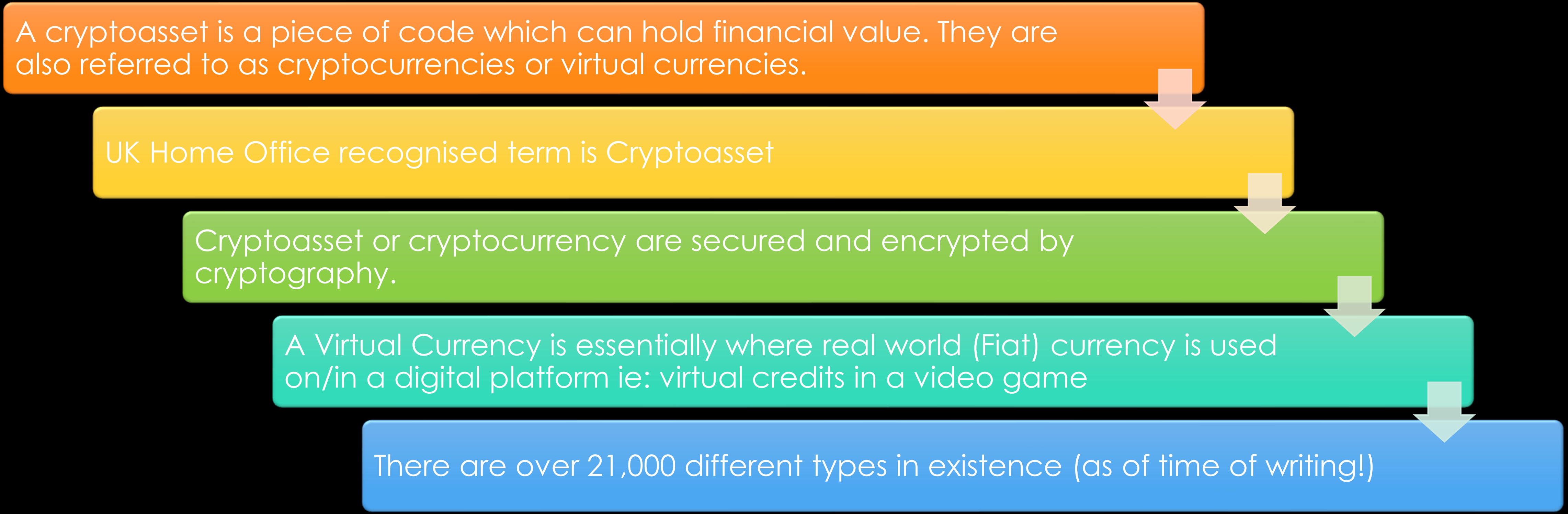
- A Consensus Mechanism is a method for validating entries into a DLT data base securely
- PoS – created as alternative to PoW
- Requires validators to hold and stake tokens for the privilege of earning transaction fees
- Next block writer (node) is selected at random
- Blocks are validated by several nodes not just one, who agree that it is accurate
- When the validation number reaches a specific number the block is final and closed
- The larger the stake position the higher the odds of being selected
- Considered less risky due to the way is structures compensation payments
- Less computational work = Less energy consumed
- Ethereum requires 32 ETH staked.
- Validation Pools use liquid staking using ERC-20 token to represent your ETH

PROOF OF STAKE V PROOF OF WORK



Proof of Stake	Proof of Work
Block creators are called validators	Block creators are called miners
Participants must own coins or tokens to become a validator	Participants must buy equipment and energy to become a miner
Energy efficient	Not energy efficient
Security through community control	Robust security due to expensive upfront requirement
Validators receive transactions fees as rewards	Miners receive block rewards

SO WHAT ARE CRYPTOASSETS?



A cryptoasset is a piece of code which can hold financial value. They are also referred to as cryptocurrencies or virtual currencies.

UK Home Office recognised term is Cryptoasset

Cryptoasset or cryptocurrency are secured and encrypted by cryptography.

A Virtual Currency is essentially where real world (Fiat) currency is used on/in a digital platform ie: virtual credits in a video game

There are over 21,000 different types in existence (as of time of writing!)

DIFFERENT TYPES OF TOKEN

Utility Token – used to access services of a particular protocol within a specific eco-system

Transactional/Payment Tokens – ie: Bitcoin, Ripple, etc. Function like traditional Fiat currencies.

Security Token – linked to off-chain assets, property, payable invoices, equipment, stocks and shares investments

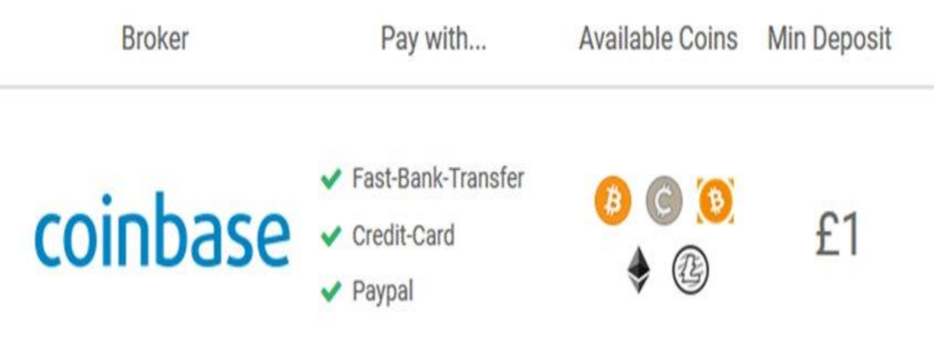
Platform Token – these deliver dapps for different usage on blockchain infrastructure – gaming, collectibles, advertising

Governance Token – allow blockchain based voting systems and are used to vote on proposals and support proposed changes

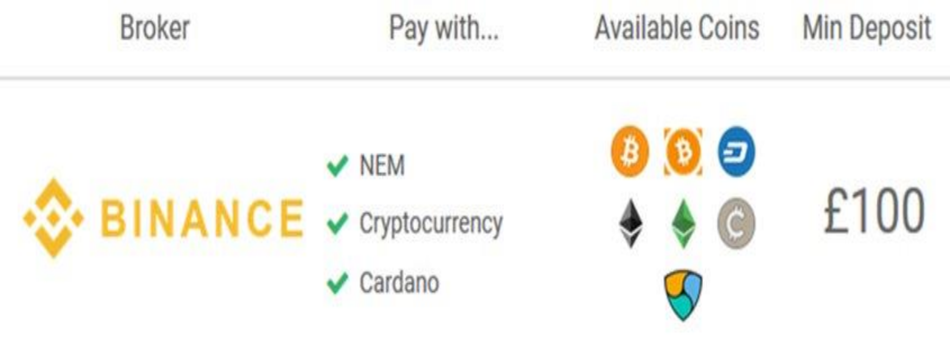
SO HOW CAN I BUY SOME CRYPTOASSETS?

- Custodial Exchange
- ATM
- Face to Face/Peer-2-Peer

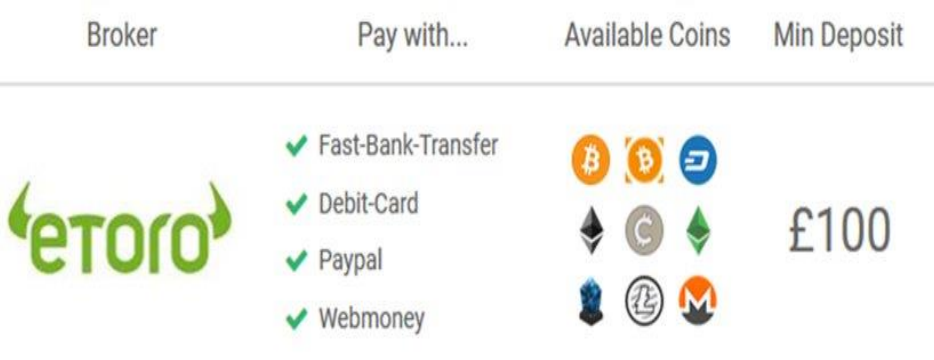
CUSTODIAL EXCHANGES



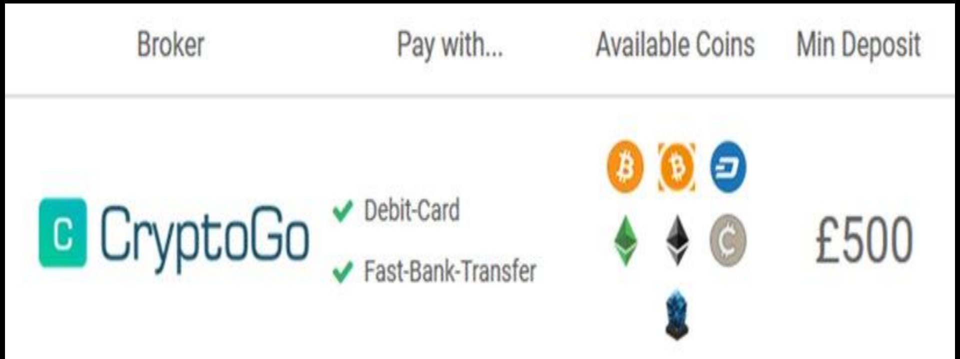
Broker	Pay with...	Available Coins	Min Deposit
coinbase	✓ Fast-Bank-Transfer ✓ Credit-Card ✓ Paypal	₿ C ₿ ◆ Ł	£1



Broker	Pay with...	Available Coins	Min Deposit
BINANCE	✓ NEM ✓ Cryptocurrency ✓ Cardano	₿ ₿ D ◆ ◆ C ●	£100



Broker	Pay with...	Available Coins	Min Deposit
eToro	✓ Fast-Bank-Transfer ✓ Debit-Card ✓ Paypal ✓ Webmoney	₿ ₿ D ◆ C ◆ ● Ł M	£100



Broker	Pay with...	Available Coins	Min Deposit
C CryptoGo	✓ Debit-Card ✓ Fast-Bank-Transfer	₿ ₿ D ◆ ◆ C ●	£500

CRYPTO ATMS

- Similar to normal ATM
- Pay in cash
- Upload crypto to your wallet
- CoinATMradar.com

FACE TO FACE

CAN BE VERY FAST

CAN BE ANONYMOUS = NO IDENTITY VERIFICATION REQUIRED

NO NEED TO TO GIVE YOUR REAL NAME, ADDRESS, ETC

- Is the other person trustworthy?
- Are you able to purchase/sell for a reasonable market value?
- Can you agree on a payment method?
- Can you name all the different types of payment methods accepted by LocalBitcoins.com?

BREAKOUT GROUPS

Cash in person

Cash deposit

Cash by mail

National bank transfer

SEPA (EU) bank transfer

Transfers with specific bank

SWIFT – International Wire

Paypal

Moneybookers/Skrill

WebMoney

Venmo

Vanilla

Telegramatic Order

Interac e-transfer

Alipay

Superflash

Chase Quickpay

OKPay

Neteller

Western Union

PostePay

Moneygram

Postal Order

Cashier’s Cheque

Transferwise

Pingit

Dwolla

Perfect money

Ukash

CashU

PaySafeCard

MoneyPak

Payza

EgoPay

AstroPay

M-PESA Kenya (Safaricom)

M-PESA Tanzania (Safaricom)

SolidTrustPay

BUT WHERE WILL I STORE THEM?

Custodial Wallet – held with an exchange

Desktop Wallet – software stored on your computer

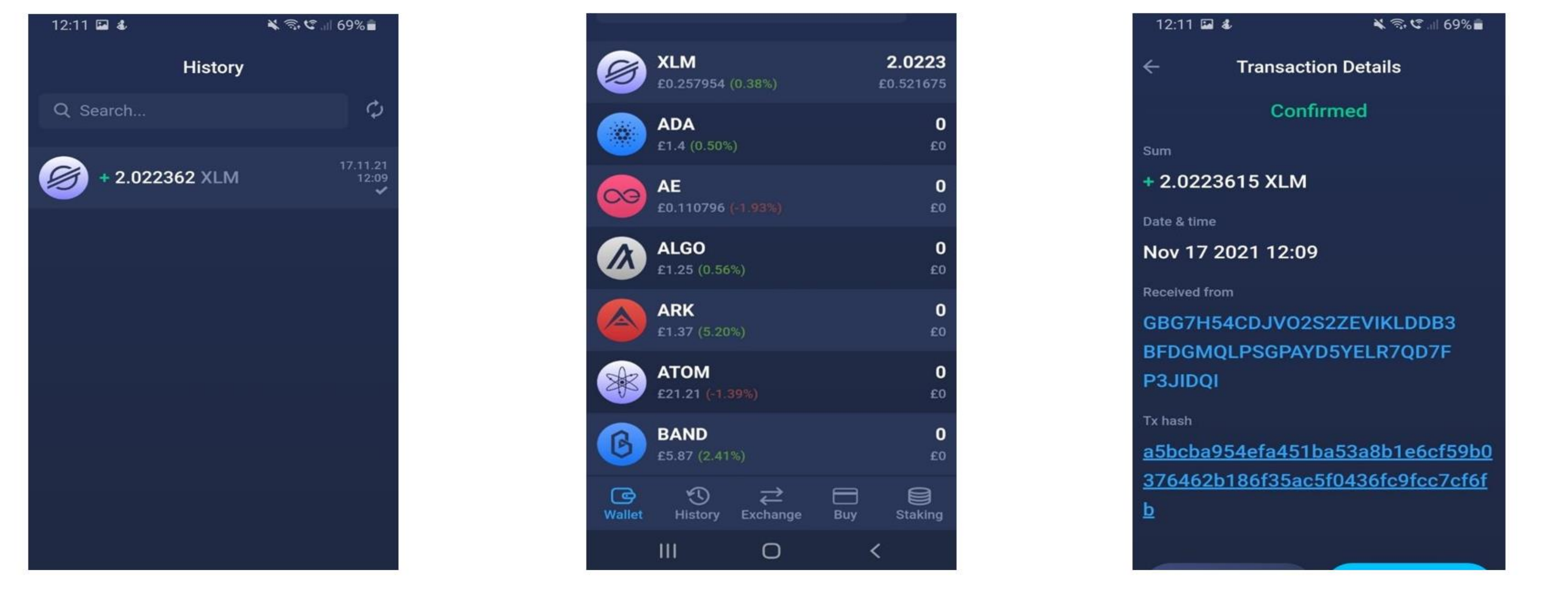
Web based wallet – software through your browser

Mobile wallet – software for your phone

Hardware wallet – specifically designed device

Paper wallet – printed record of public & private keys

MOBILE/ONLINE/DESKTOP WALLETS



12:11 69%

History

Search...

+ 2.022362 XLM 17.11.21 12:09

XLM £0.257954 (0.38%)	2.0223 £0.521675
ADA £1.4 (0.50%)	0 £0
AE £0.110796 (-1.93%)	0 £0
ALGO £1.25 (0.56%)	0 £0
ARK £1.37 (5.20%)	0 £0
ATOM £21.21 (-1.39%)	0 £0
BAND £5.87 (2.41%)	0 £0

12:11 69%

Transaction Details

Confirmed

Sum

+ 2.0223615 XLM

Date & time

Nov 17 2021 12:09

Received from

GBG7H54CDJVO2S2ZEVIKLDDB3BFDGMQLPSGPAYD5YELR7QD7FP3JIDQI

Tx hash

a5bcba954efa451ba53a8b1e6cf59b0376462b186f35ac5f0436fc9fcc7cf6fb

keep
key
RECOVERY SENTENCE
1.power 2.speak 3.east 4.detail 5.pitch
6.debate 7.page 8.solid 9.point 10.you
11.cart 12.cinnamon
Bac

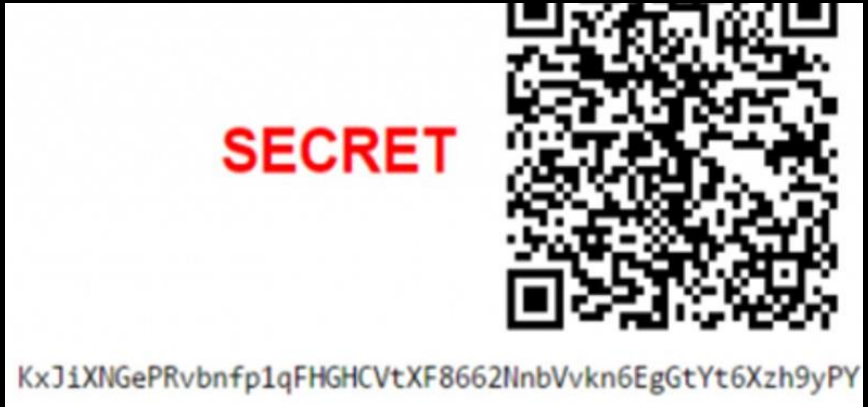
HARDWARE WALLET TYPES

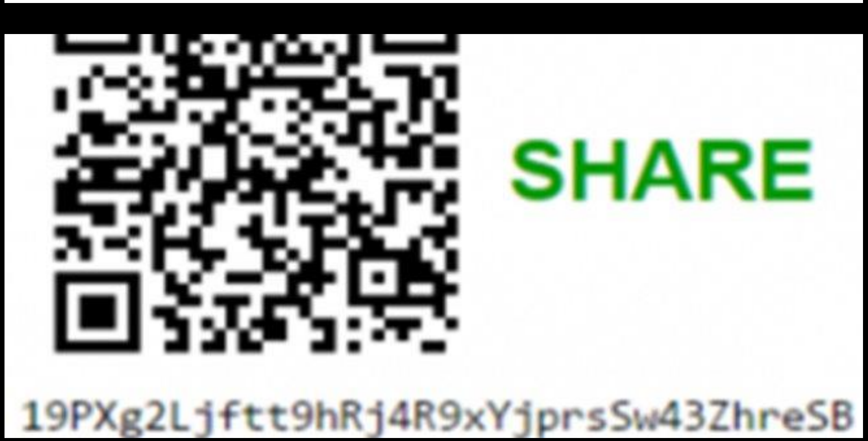
PUBLIC ADDRESS
bitcoin
DEPOSIT / VERIFY
aBcDeFgHiJkLmNoPqRsTuVwXyZ1234567890
PRIVATE KEY / WITHDRA

PAPER WALLET

SO HOW DO I USE MY CRYPTOS?

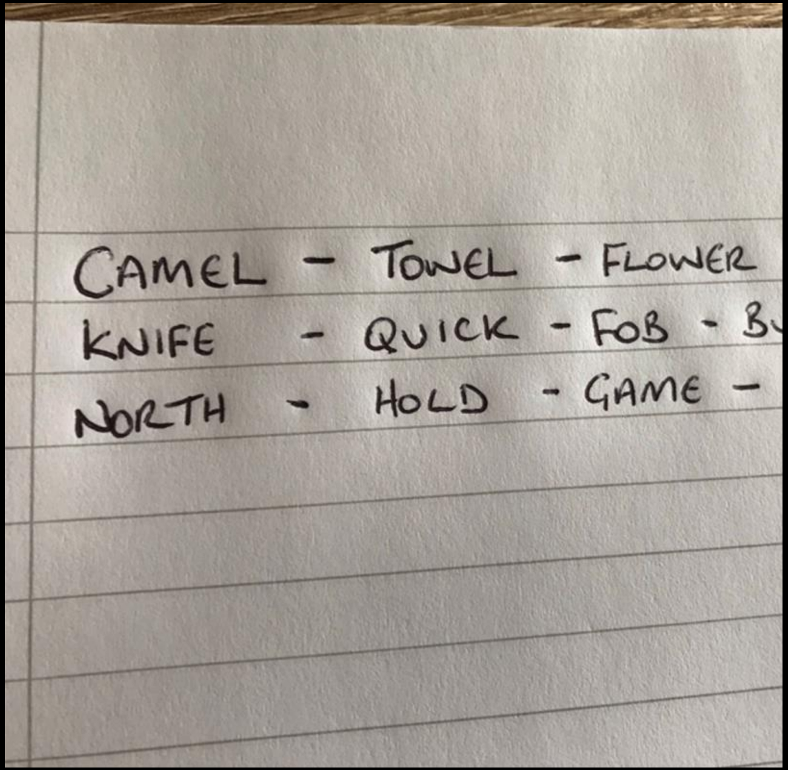
- Public Key – This you share like your sort code and account number to receive payments
- Private Key – This you use to sign/confirm your transactions when you are sending cryptos
- If you have someone’s private key then you have control of their crypto wallet
- If you lose your private key then you lose your cryptos ....unless ...





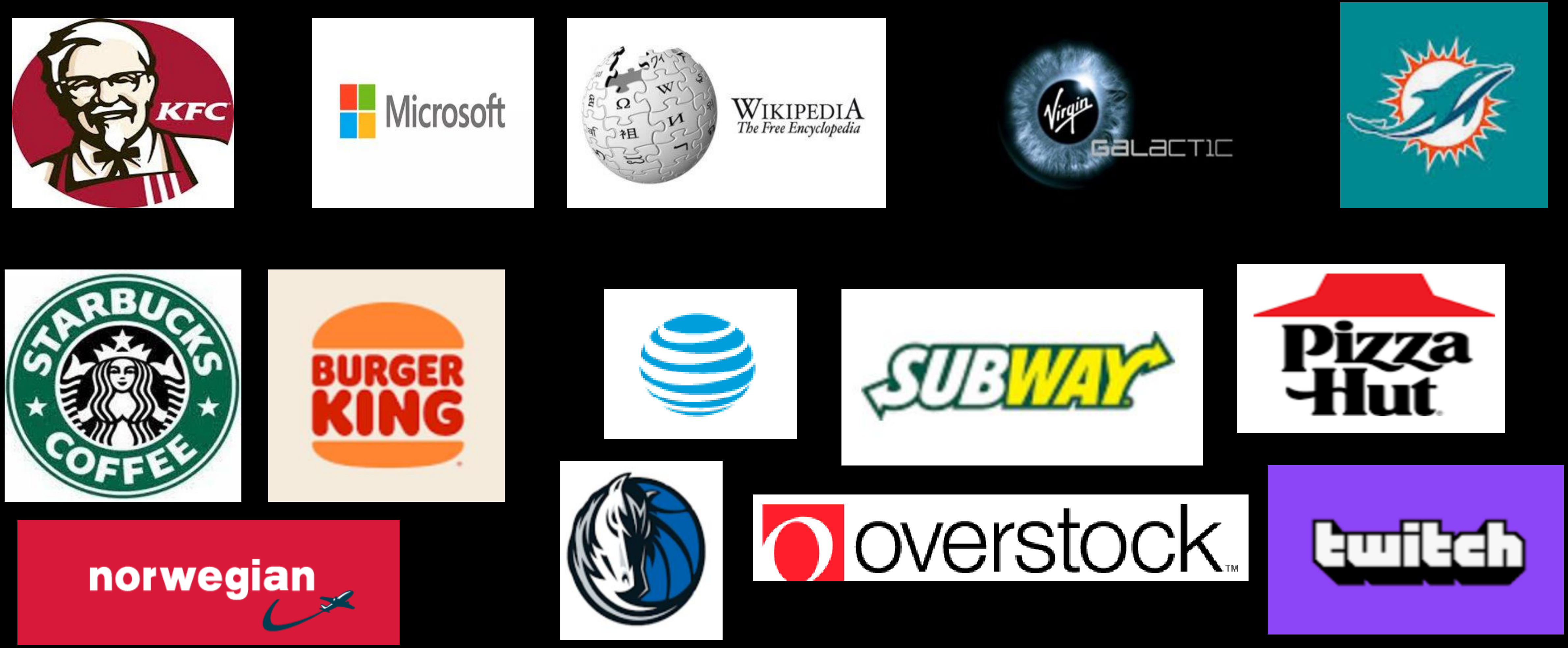
RECOVERY SEED OR RECOVERY PHRASE

- This is a readable interpretation of the alpha-numeric string of your private key
- Can be anywhere between 12 and 24 words long
- If you have control or sight of this then you can recreate that wallet on a different device or in a different wallet

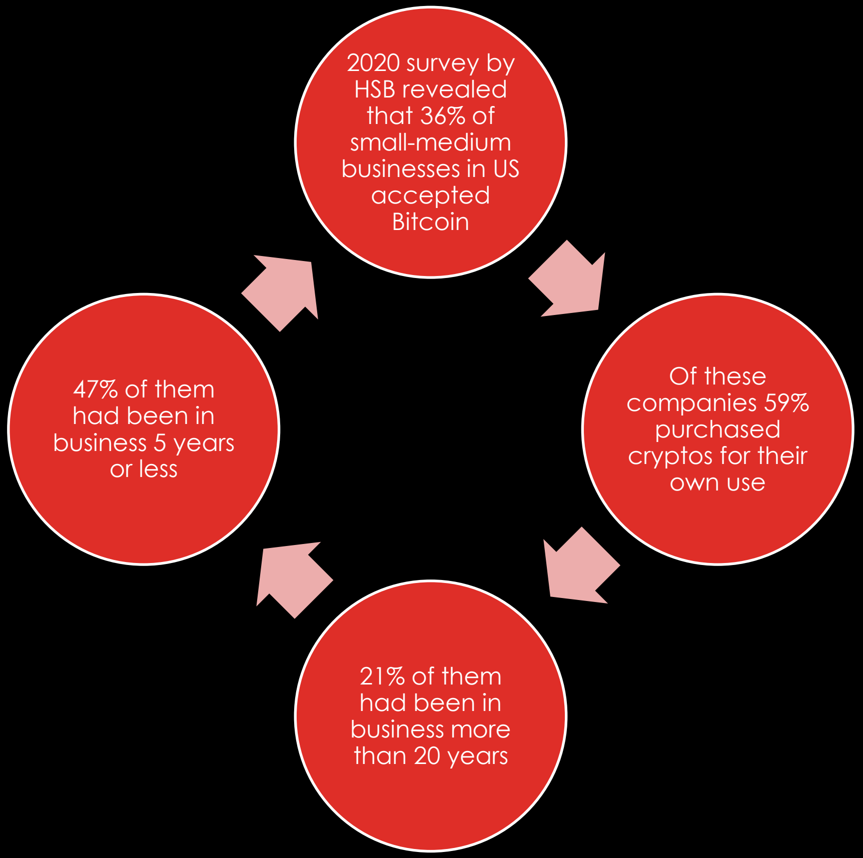


CAMEL - TOWEL - FLOWER
KNIFE - QUICK - FOB - B
NORTH - HOLD - GAME -

SO WHERE CAN I SPEND MY BITCOINS?



WHAT ABOUT SMALLER BUSINESSES?



2020 survey by HSB revealed that 36% of small-medium businesses in US accepted Bitcoin

Of these companies 59% purchased cryptos for their own use

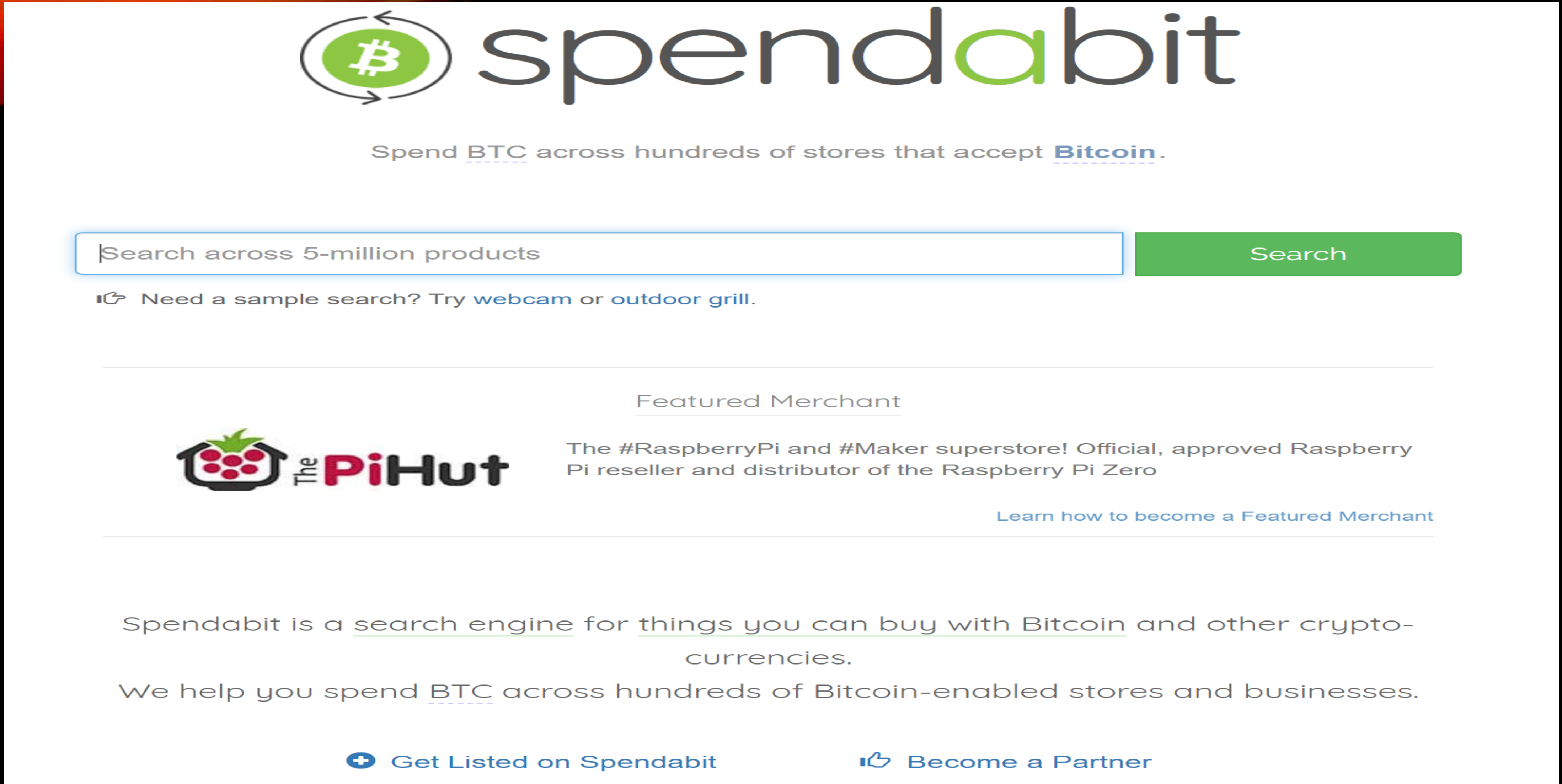
21% of them had been in business more than 20 years

47% of them had been in business 5 years or less

- Benefits
- Lower fees on process
- Faster payments
- Potentially a source of off-book income? (not through a till)
- Drawbacks
- Increased risk of computer hacks
- Cyber fraud via malware

ANY OTHER WAYS TO SPEND MY CRYPTOS?

- Bitcoin debit cards (also Litecoin & Ethereum supported)
- Make on-line or in-person purchases
- Withdraw cash from ATMs (even non-crypto ATMS)
- Pre-loaded with set amount of crypto
- Automatically converted at time of purchase
- Often offer other rewards – cashback, mobile apps
- Other Vendors – Wirex, Blockcard, Nuri, Crypto.com



Spendabit

Spend BTC across hundreds of stores that accept Bitcoin.

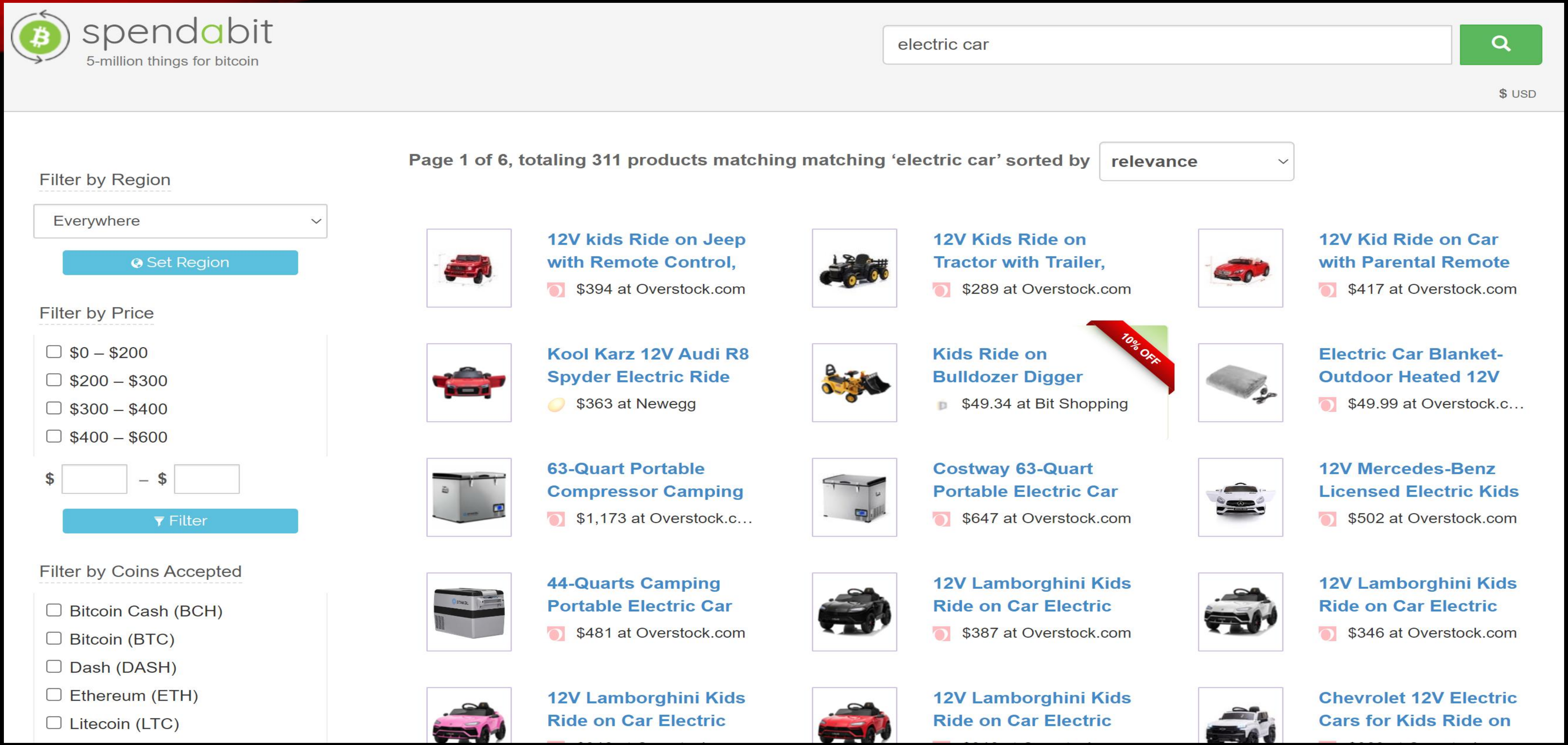
Need a sample search? Try webcam or outdoor grill.

Featured Merchant

The #RaspberryPi and #Maker superstore! Official, approved Raspberry Pi reseller and distributor of the Raspberry Pi Zero

Learn how to become a Featured Merchant

Spendabit is a search engine for things you can buy with Bitcoin and other crypto-currencies.
We help you spend BTC across hundreds of Bitcoin-enabled stores and businesses.



spendabit
5-million things for bitcoin

electric car

$ USD

Filter by Region

Everywhere

Set Region

Filter by Price

- □ $0 – $200
- □ $200 – $300
- □ $300 – $400
- □ $400 – $600

$ ____ – $ ____

Filter

Filter by Coins Accepted

- □ Bitcoin Cash (BCH)
- □ Bitcoin (BTC)
- □ Dash (DASH)
- □ Ethereum (ETH)
- □ Litecoin (LTC)

Page 1 of 6, totaling 311 products matching matching 'electric car' sorted by relevance

12V kids Ride on Jeep with Remote Control,
$394 at Overstock.com

12V Kids Ride on Tractor with Trailer,
$289 at Overstock.com

12V Kid Ride on Car with Parental Remote
$417 at Overstock.com

Kool Karz 12V Audi R8 Spyder Electric Ride
$363 at Newegg

Kids Ride on Bulldozer Digger
$49.34 at Bit Shopping

10% OFF

Electric Car Blanket-Outdoor Heated 12V
$49.99 at Overstock.c...

63-Quart Portable Compressor Camping
$1,173 at Overstock.c...

Costway 63-Quart Portable Electric Car
$647 at Overstock.com

12V Mercedes-Benz Licensed Electric Kids
$502 at Overstock.com

44-Quarts Camping Portable Electric Car
$481 at Overstock.com

12V Lamborghini Kids Ride on Car Electric
$387 at Overstock.com

12V Lamborghini Kids Ride on Car Electric
$346 at Overstock.com

12V Lamborghini Kids Ride on Car Electric

12V Lamborghini Kids Ride on Car Electric

Chevrolet 12V Electric Cars for Kids Ride on

SO WHERE DOES THAT LEAVE LAW ENFORCEMENT AGENCIES?

Cannot trace transactions using standard ML methods and tools

Insufficient tools available

How do you go about attributing a specific wallet to an individual?

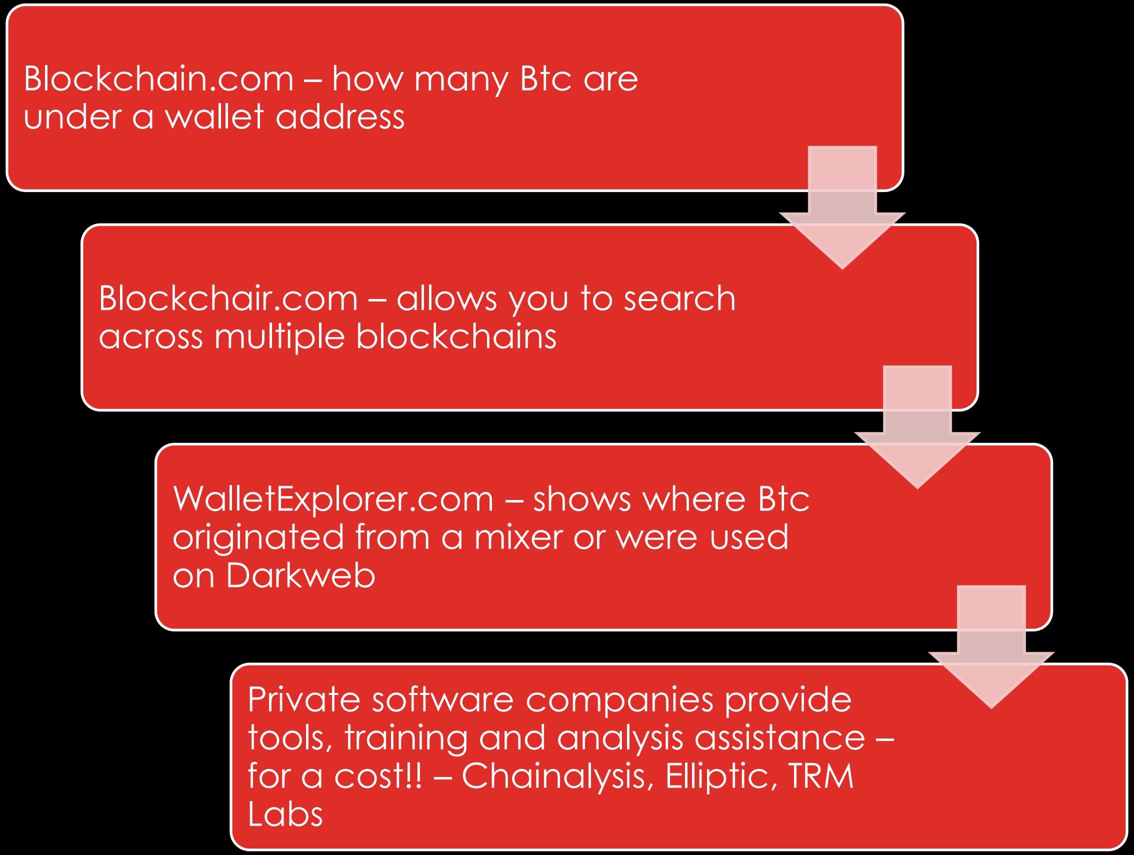
How do you obtain information from an exchange?

How do you know where an exchange is based?

Is the legislation in place to allow you to trace transactions?

- Is the legislation in place to allow you to seize Cryptoassets?
- What open source tools can give you the best help?
- Who do I go to for assistance?
- Who has the expertise?
- Who could present this in court and explain it to a judge and jury?
- If I find a wallet how can I get access to it?

CONDUCTING AN INVESTIGATION



Blockchain.com – how many Btc are under a wallet address

Blockchair.com – allows you to search across multiple blockchains

WalletExplorer.com – shows where Btc originated from a mixer or were used on Darkweb

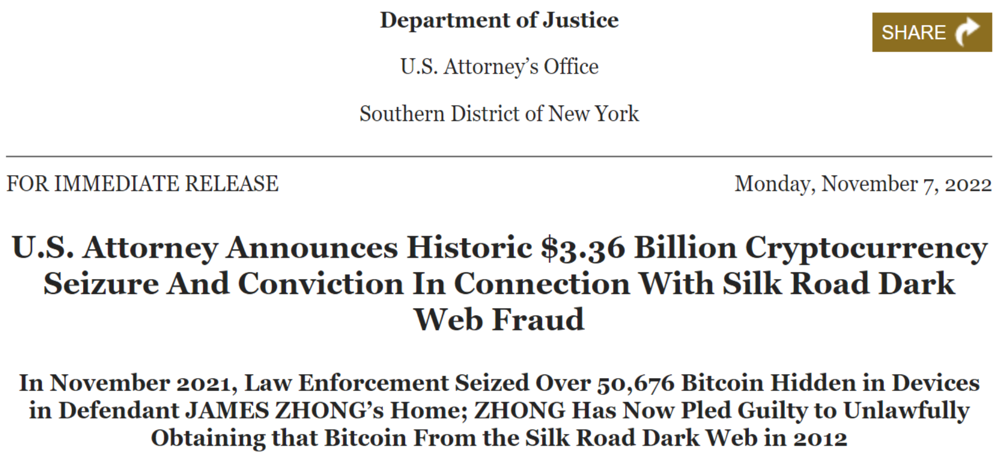
Private software companies provide tools, training and analysis assistance – for a cost!! – Chainalysis, Elliptic, TRM Labs

- OCGs use TOR network or other ways to mask IP addresses
- Use of mixers or tumblers
- Dark Wallets anonymise transactions
- Hardware and E-wallets come with plausible deniability mechanisms added – hidden wallets attached to visible ones
- Customised “white label” services – to create own Crypto exchange – infrastructure and software

THE SEIZURE PROCESS CONSIDERATIONS

- What legal basis exists to allow you to undertake a seizure?
- Practical basis – how are you physically going to take control of it?
- Risk – movement from a criminal wallet into a government-controlled wallet
- Risk – Temptation or Corruption – how do you lessen risks? Support you staff?
- Risk – Where will you store the seized Cryptoassets?
- What technology is available to you to use?
- What supporting infrastructure is there for the technology?
- On ground seizures – USA, Australis
- Remote seizure – UK HMRC FIS approach

DOES IT WORK?



Department of Justice

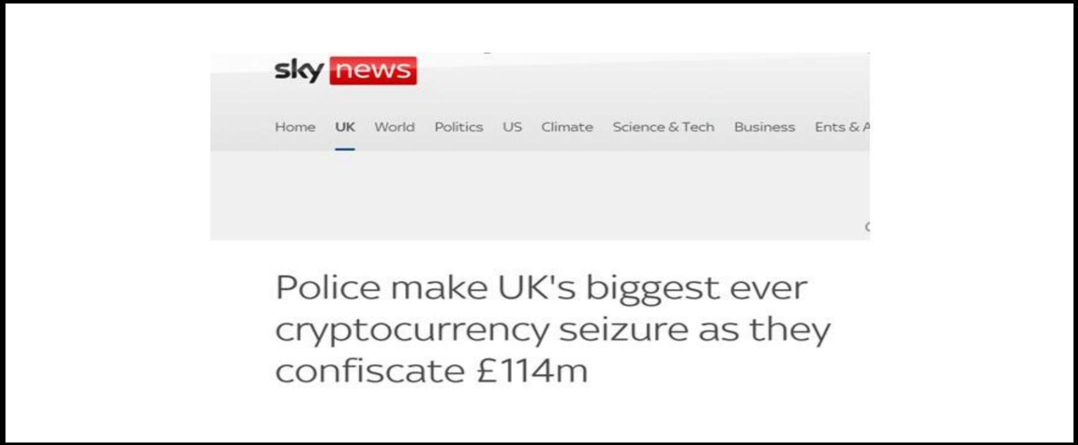
U.S. Attorney's Office

Southern District of New York

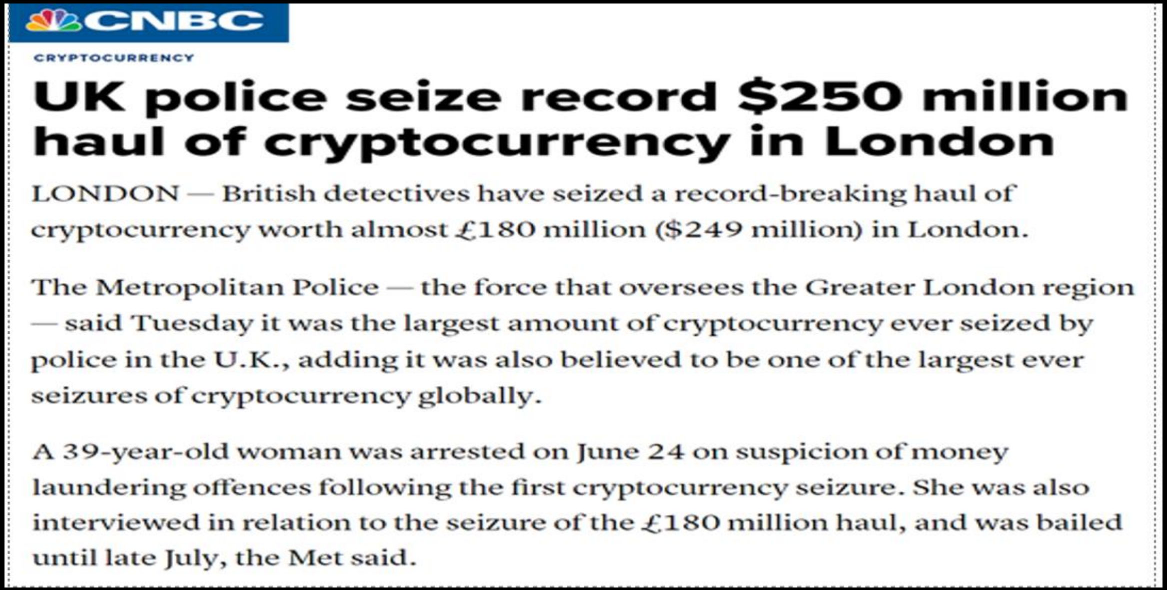
FOR IMMEDIATE RELEASE Monday, November 7, 2022

U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud

In November 2021, Law Enforcement Seized Over 50,676 Bitcoin Hidden in Devices in Defendant JAMES ZHONG's Home; ZHONG Has Now Pled Guilty to Unlawfully Obtaining that Bitcoin From the Silk Road Dark Web in 2012



Police make UK's biggest ever cryptocurrency seizure as they confiscate £114m

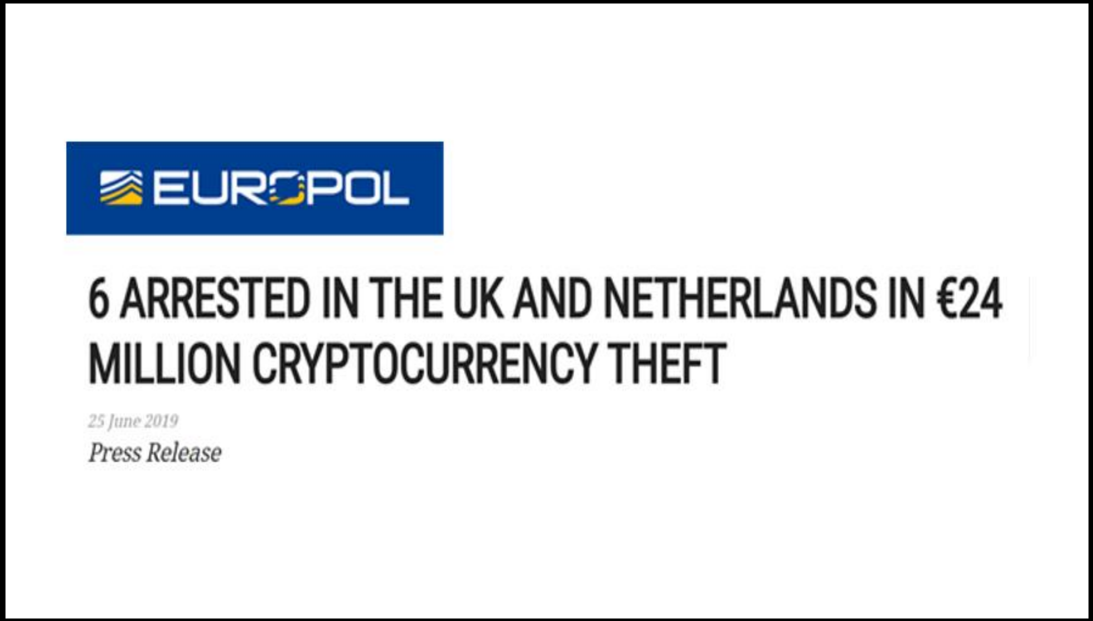


UK police seize record $250 million haul of cryptocurrency in London

LONDON — British detectives have seized a record-breaking haul of cryptocurrency worth almost £180 million ($249 million) in London.

The Metropolitan Police — the force that oversees the Greater London region — said Tuesday it was the largest amount of cryptocurrency ever seized by police in the U.K., adding it was also believed to be one of the largest ever seizures of cryptocurrency globally.

A 39-year-old woman was arrested on June 24 on suspicion of money laundering offences following the first cryptocurrency seizure. She was also interviewed in relation to the seizure of the £180 million haul, and was bailed until late July, the Met said.



6 ARRESTED IN THE UK AND NETHERLANDS IN €24 MILLION CRYPTOCURRENCY THEFT

25 June 2019

Press Release

GREG KELLY
CRYPTOASSET SME
TECHNOLOGY ENABLED MONEY LAUNDERING TEAM
ILLICIT FINANCE STRATEGY
HMRC FRAUD INVESTIGATION SERVICE

greg.kelly@hmrc.gov.uk

Mobile - 07825546060