CRYPTOASSETS – THE IMPLICATIONS FOR LAW ENFORCEMENT AGENCIES

- INTRODUCTION

- Cryptoassets began as an attempt to secure greater privacy from financial intermediaries and governments in financial transactions

- Cryptoassets have the potential to cause an important structural shift in how the Black market operates

UK – ATTITUDES & AWARENESS OF CRYPTOASSETS

- October 2018 – Financial Conduct Authority published a joint report alongside Bank of England and HM Treasury as part of UK domestic taskforce on cryptoassets.
- Sets out UK's Policy and Regulatory approach to Cryptoassets and DLT
- Identified 3 major risks of harm to market integrity, financial crime and consumers – but identified a lack of credible evidence on consumer usage
- Commissioned 2 research pieces
- First using 31 Cryptoasset consumers – two sets of interviews
- Second using 2,132 UK consumers – high level questions

RESEARCH GROUP 1

PURCHASE

USAGE

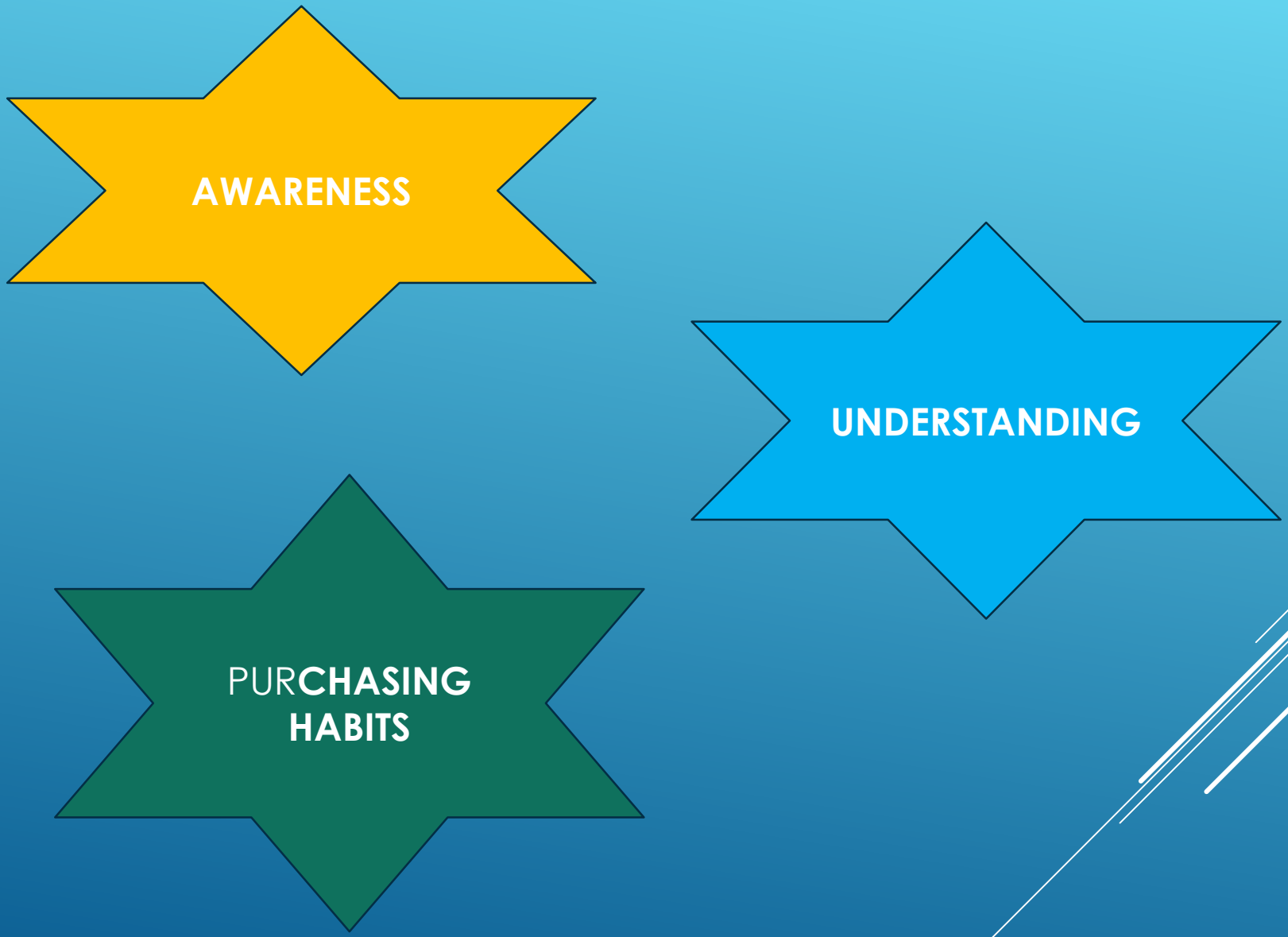
ATTITUDES

BELIEFS

MOTIVATION

UNDERSTANDING

RESEARCH GROUP 2



FINDINGS

1 Consumers purchasing cryptoassets looking for way to "get rich quick"

2 Many consumers did not understand what they were buying

3 Associated with Risky Behaviours

Anecdotal evidence may overstate harm -

73% did not know what a cryptocurrency was or could define it

Term most recognised by males – 20 to 44 years old (middle class & upper middle class)

Only 3% of surveyed had ever bought it Half of those who purchase spend under £200

All used own money – none borrowed

Those who had not bought are unlikely to do so – only 1 in 100 were going to buy in future

WHAT IS BLOCKCHAIN AND HOW DOES IT WORK?

- Blockchain is a type of Distributed Ledger Technology (DLT)
- Financial institutions operate around "Centralised Ledgers" (1)
- No formal definition of a DLT (2)
- Instead of relying on one source you have a group of peers who maintain a shared database. The consensus of the group is the record.
- Benefit ? Less vulnerable to hacking or tampering (3)
- Each transaction forms a block. Blocks are "chained" together through a complex mathematical algorithm.
- A block can only be created when all peers agree and each new block receives a unique digital signature. (4)
- Customer information can be coded but each transaction would be available to see by all participants
- Positives of Blockchain – lowers the cost of transactions, removes middlemen – potentially speeds up the process
- Negatives – it is slow and it can take time to add to the ledger
- Could Blockchain assist in the fight against Financial Crime? (5)
- Future of DLT (6)

ADVANTAGES OF BLOCKCHAIN

- Secure Real Time Payment – wire transfers can take days, hugely inefficient. Blockchain enabled payments – instant. Effective service
- Reduce Contract Fraud – a contract embedded in digital code. Transparent, shared, protected from tampering, reduces corruption
- Transaction Guarantee – once embedded in code the smart contract is fulfilled and the counter party is paid. No need to chase debtors
- Increased efficiency in supply chains - companies and vendors - view available inventory and track it all the way to a customer
- Security Internet of Things – smart home technology customers should have added comfort over security provided by Blockchain use. Increase advance in this area.
- Improved Credit Ratings for small businesses – Blockchain accounting software provides trust for 3rd parties via transparency. Increased lending opportunities without significant costs
- Reduce Carbon Footprint – smart contracts on Blockchain means less paper printed

INTRODUCTION TO CRYPTOASSETS

- Historical use of Cryptocurrencies – Darknet (DarkWeb)
- Drop in use of Bitcoins 2017 – from 30% to under 1% on Dark web sites
- Move into Money Laundering arena – driven by what?
- Diversification
- Perception
- LEA Knowledge
- Lack of Global Regulation
- Trackability
- Wider audience adoption

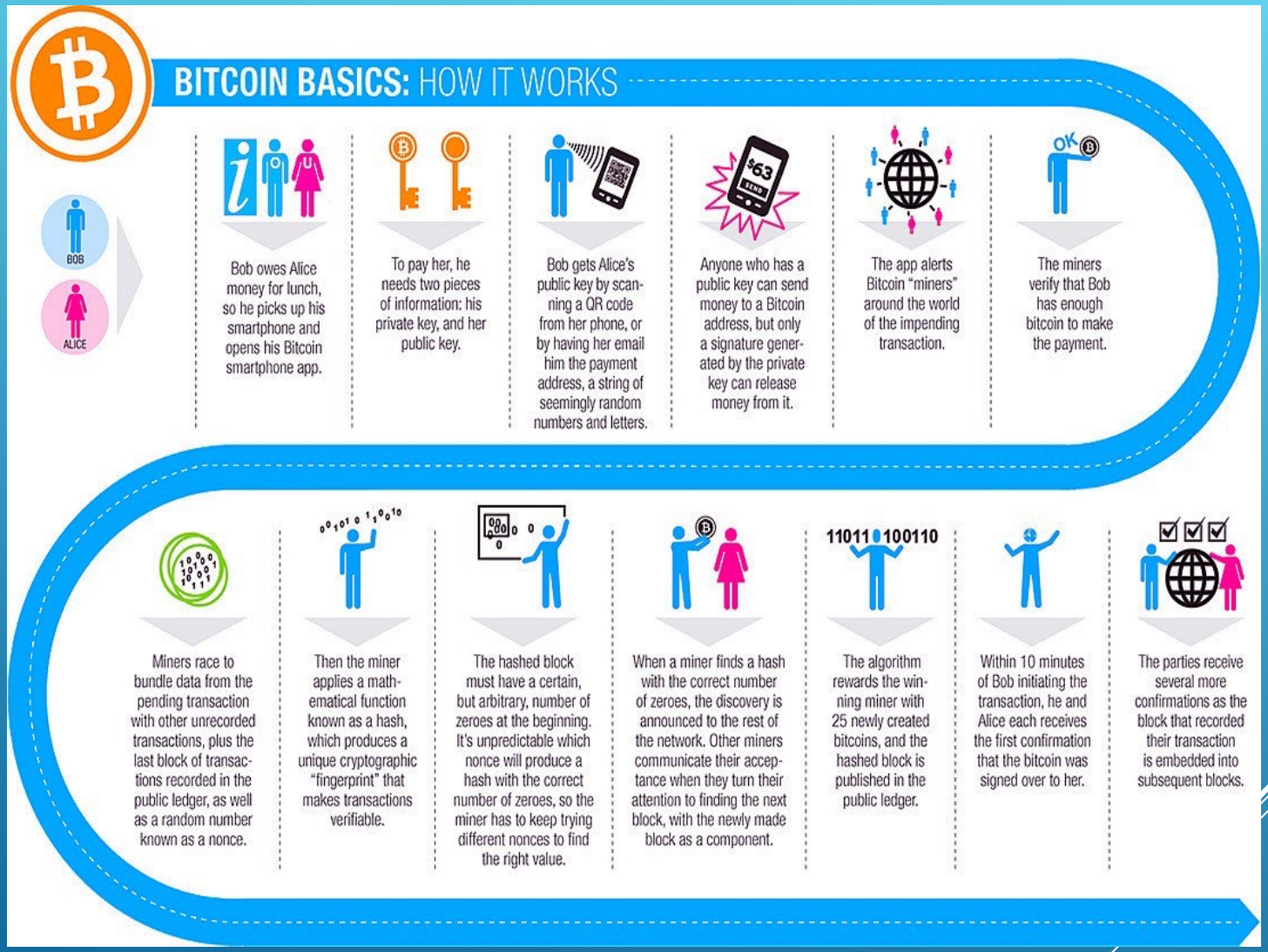
WHY WOULD CRIMINALS USE A CRYPTOASSET?

- 1 - Purchase of illegal goods or services on the Dark Web – Bitcoin was always the "currency" of choice. Overtaken by more anonymous Cryptoassets. (1)
- Purchase of firearms, drugs, people, contract killings, etc
- 2 – Storage of illicitly generated funds outside of traditional banking arena.
- 3 – Ease of use as it can be mobile and carried with you wherever you go.
- 4 – Transfer of Money – large amounts can be sent anywhere in the world at the press of a button. No regulation or controls in place. Low cost.
- Bitcoin is often the Cryptoasset of choice for Ransomware or Sextortion

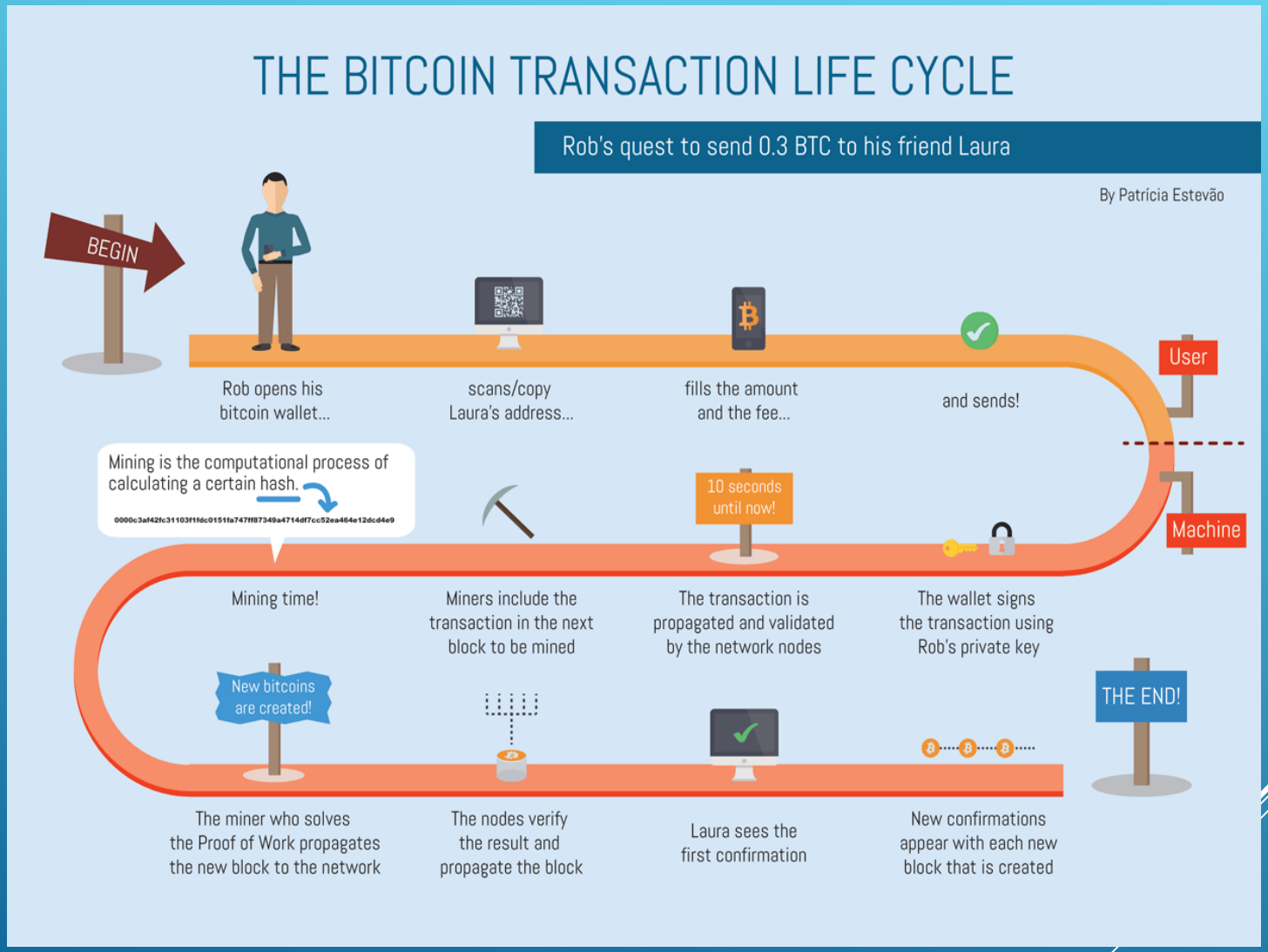
BITCOIN BASICS- HOW IT WORKS

- Users need a *wallet* in which to store/ receive bitcoin.
- The wallet creates your bitcoin address (like an email address) and keeps a secret piece of data called a *private key*.
- The private key is used to sign transactions. This provides proof that they have come from the owner of the wallet.
- A transaction is *a transfer of value* between bitcoin wallets that gets included in the block chain
- The blockchain is a public ledger showing all confirmed transactions
- Transactions are confirmed by *miners* who effectively manage and test the cryptography

OFFICIAL


BITCOIN BASICS: HOW IT WORKS
BOB
ALICE
Bob owes Alice money for lunch, so he picks up his smartphone and opens his Bitcoin smartphone app.
To pay her, he needs two pieces of information: his private key, and her public key.
Bob gets Alice's public key by scanning a QR code from her phone, or by having her email him the payment address, a string of seemingly random numbers and letters.
$63
SEND
Anyone who has a public key can send money to a Bitcoin address, but only a signature generated by the private key can release money from it.
The app alerts Bitcoin "miners" around the world of the impending transaction.
OK
The miners verify that Bob has enough bitcoin to make the payment.
Miners race to bundle data from the pending transaction with other unrecorded transactions, plus the last block of transactions recorded in the public ledger, as well as a random number known as a nonce.
Then the miner applies a mathematical function known as a hash, which produces a unique cryptographic "fingerprint" that makes transactions verifiable.
The hashed block must have a certain, but arbitrary, number of zeroes at the beginning. It's unpredictable which nonce will produce a hash with the correct number of zeroes, so the miner has to keep trying different nonces to find the right value.
When a miner finds a hash with the correct number of zeroes, the discovery is announced to the rest of the network. Other miners communicate their acceptance when they turn their attention to finding the next block, with the newly made block as a component.
11011 100110
The algorithm rewards the winning miner with 25 newly created bitcoins, and the hashed block is published in the public ledger.
Within 10 minutes of Bob initiating the transaction, he and Alice each receives the first confirmation that the bitcoin was signed over to her.
The parties receive several more confirmations as the block that recorded their transaction is embedded into subsequent blocks.

OFFICIAL


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
10 seconds until now!
Mining time!
Miners include the transaction in the next block to be mined
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
THE END!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created

OFFICIAL

WHAT DO WE MEAN BY CRYPTOASSETS?

- A digital token created using cryptography which allows for it to be generated, stored, and transacted securely and, most commonly, anonymously.
- Generally decentralised and use Distributed Ledger Technology – records transactions in multiple places at the same time no central data store
- Blockchain is a DLT format – which operates outside of the standard banking systems
- Developed as code with built in mechanisms for issuance (often, although not always, through a process called "mining") and other controls.
- They are governed a value by the market of supply and demand
- They are generally designed to be free from government manipulation and control. (The rise in popularity and usage has lead to this particular aspect coming under attack from certain governments and institutions).
- Bitcoin (BTC) was the first one launched in 2009.
- Currencies introduced after BTC, claim that they are modified or improved versions of BTC. They are also referred to as Altcoins.
- Benefits of Altcoins - easier to mine than BTC, more anonymity.
- Drawbacks – greater risk on investment – due to lesser acceptance and value retention. Liquidity of asset

CRYPTOASSET BASICS

- They can be convertible or non-convertible (used in closed environment) [1]
- Acquired from an online exchange – fiat currency for CC [2]
- Face to face for cash – localbitcoins.com
- Bitcoin ATM – for cash or card payments
- CC wallet providers hold the CC on behalf of their customers [3]
- They store CCs and allow for transfers to other wallets or CC accounts
- BTC address and BTC Wallet are not linked to a name or identity
- Exchanges – brokers between "real" and virtual worlds – offer ways to buy or sell CCs for a fee. Also exchange CCs in formats.
- Services – Fiat to Crypto, Crypto to Fiat, Crypto to Crypto
- Exchanges – not regulated in a co-ordinated fashion in EU
- Other Storage – Electronic devices or removable media (phone, laptops, USB thumb drives, SD cards, etc), Paper wallets, Hardware wallets [4]
- In order to transfer/control BTC you need to have the private key/recovery seed

HOW WOULD YOU GO ABOUT PURCHASING A CRYPTOASSET?

- Step 1 – download a wallet app to your phone – Coinbase and Blockchain.info. This is where you will store your coins and also from where you will conduct your transactions
- Step 2 – once the wallet is downloaded it will generate an address. It can be used as a bank account in effect
- Step 3 – Now you are free to buy Cryptoassets in one of 3 ways:
- ATMs – these are limited to specific cryptoassets only currently. Put cash in, scan your phone and store value in your wallet
- Face to Face – various websites offer services for these transactions. Mainly Bitcoin.
- Exchanges – legitimate websites. Sign up and pay with debit/credit card or bank transfer. Most of these will require you to provide identification.
- Gift cards – More later

CUSTODIAN WALLET VS LIGHT WALLET

- First decision is your wallet – Custodian or Light (Non-Custodial)
- Custodial – your private keys are held by 3rd party. You do not have full control over your crypto. Bit like a bank – they hold your funds.
- Advantages – you cannot lose your private keys. You can access your funds from anywhere with internet
- Disadvantages – the Custodian controls your funds. If your wallet gets hacked you could lose all your funds. If there is a fork you might not receive your funds. If the Custodian is compliant (5th AMLD) your funds could be frozen and seized under a court order
- Freewallet – platform – users can create mobile cryptoasset wallets to work with tokens. Multiple cryptoasset options. In 2017 complaints that Freewallet had sent their money to unknown addresses.
- Blockchain.info - partially centralized wallet. Has suffered some major thefts—February 2018, hackers stole 700 BTC
- BTC.com—first mobile service designed for tablets & smartphones. Clients connect directly to the Bitcoin network - confidential data more secure and no access to funds by third parties.

CUSTODIAL EXCHANGES

- You store your funds in a wallet on their platform
- **Coinbase**— the largest exchange for trading cryptos. One of the few whose own accounts have never been hacked
- **Bitfinex** - is one of the largest cryptocurrency-related fintech companies. But in 2016 hackers stole 120 000 bitcoins. Bitfinex paid out compensation
- **Poloniex**—Large crypto-exchange trading more than 100 cryptos. In 2018 attacked by scammers trying to get access to user accounts
- **Kraken**—US exchange (2F-authorisation). In 2018, some clients were victims of phishing
- **Bithumb** - Korean crypto exchange. Supports 10 cryptos. One of world leaders in trading volumes per day. In 2017 – hacked - 1.2M Korean Won stolen.
- **Cryptsy** – US crypto-exchange. Traded itcoin and litecoin. Hacked once which resulted in stolen coins $5M
- **Mt.Gox**—infamous hack $8M disappeared.
- **BTC-e**—largest Russian exchange. In July 2017 - suddenly went offline, and its director was arrested

NON-CUSTODIAL WALLET OR LIGHT WALLET

- Light – can be mobile, desktop, hardware, web or paper – you fully control your funds.
- Web based - do not keep your keys - stored in your browser. Such wallets as MyEtherWallet and Guarda allow you to access your account from any device, all you need to enter is your private key.
- Hardware - considered the most secure cryptoasset storage solution. They are similar to flash drives and do not have internet access. No in for hackers.
- Mobile Light wallets - installed on a smartphone or tablet. Vast amount of choice. Download applications from the developer's site. Also available on AppStore and Google Play – gives protection from downloading a fake application
- Desktop wallet - application installed directly on your computer. Examples - Electrum and BitGo. Only available when internet connected. Keys stored on the computer. Anyone access to the computer can access your funds.
- Paper wallets - you print your public and private keys on a piece of paper. Stored offline. To use - connect from any device and enter your keys.

USING A CRYPTOASSET

- Most are pseudo-anonymous
- Owner of the asset has two digital keys – one private, one public.
- Public key appears on DLT for all to see
- Private key is the control which allows the movement of cryptoassets in a transaction
- Both are made up of characters and are linked together via cryptographic mathematics
- The keys can be stored in a "wallet"
- If the Private key or Recovery Phrase is lost then the asset is "lost" and can no longer be accessed to use

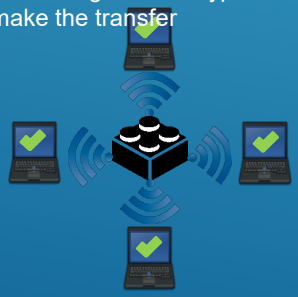
BASICS

1. A wants to send a cryptoasset to B

2. The transaction is represented online as a "block"

3. The block is broadcast to every party with access to the distributed ledger

4. Those in the network approve the transaction is valid – i.e. they all agree that A has enough of the cryptoasset available to make the transfer



5. The block then can be added to the chain, which provides an indelible and transparent record of transaction as part of that cryptoasset's history

6. The cryptoasset moves from A to B

CRYPTOCURRENCY EXCHANGE PLATFORMS

BITTREX

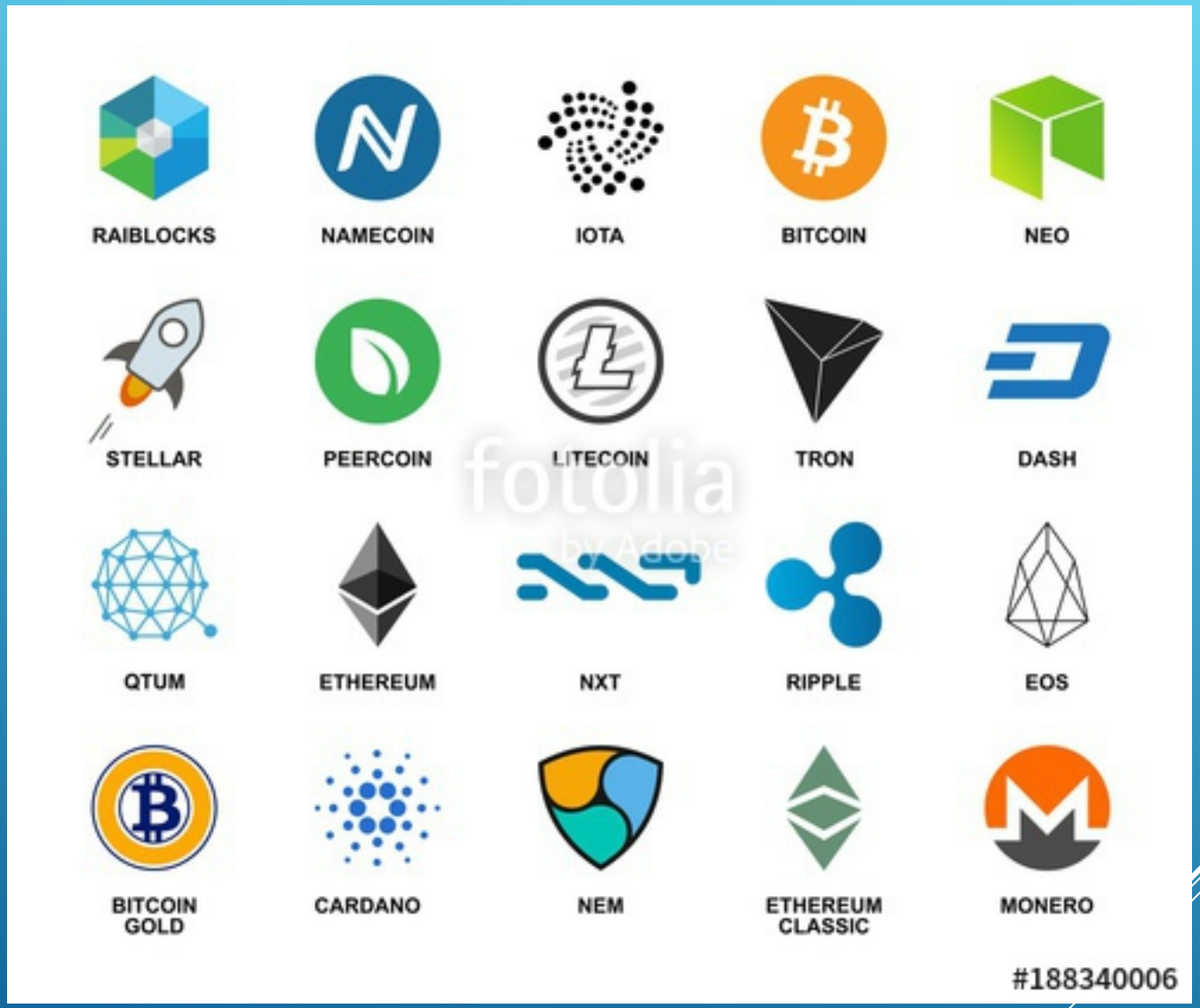
POLONIEX
CRYPTOCURRENCY EXCHANGE

kraken

bitcoin.de
Bitcoin-Marketplace - Made in Germany!

bitonic

CRYPTOASSETS MARKET



TOP 10 CRYPTOCURRENCIES (AFTER BTC)

- Litecoin (LTC) – launched 2011. MC $5.03B. TV $87.56
- Ethereum (ETH) – launched 2015. MC $47.84B. TV $474.66
- Zcash (ZEC) – launched 2016. MC $904.85M. TV $206.23
- Dash (DASH) – launched 2014. MC $2.19B. TV $266.58
- Ripple (XRP) – launched 2012. MC $19.07B. TV $0.486
- Monero (XMR) – launched 2014. MC $2.31B. TV $142.21
- Bitcoin Cash (BCH) – launched 2017. MC$14.2B. TV $827.15
- Neo (NEO) – launched 2014. MC $2.41B. TV $37.08
- Cardano (ADA) – launched 2017. MC $4.81B. TV $0.186
- Eos (EOS) – launched 2017. MC $7.65B. TV $8.53

All figures were taken as at 19TH July 2018.

TOP 10 CRYPTOASSETS (AFTER BTC)

2 Ethereum (ETH) – MC $22.711B. TV $212.22

3 Ripple (XRP) – MC $13.332B. TV $0.31

4 Litecoin (LITE) – MC $5.674B. TV $90.38

5 Bitcoin Cash (BCH) – MC $5.402B. TV $301.71

6 Binance Coin (BNB) – MC $4.589B. TV $29.50

7 Tether (USDT) – MC $4.027B. TV $1.00

8 EOS (EOS) – MC $3.812B. TV $4.12

9 Bitcoin SV (BSV) – MC $3.025B. TV $169.45

10 Stellar (XLM) – MC $1.671B. TV $0.085

12 Cardano (CDN) – MC $1.464B. TV $0.056

13 Monero (MNR) – MC $1.393B. TV $81.44

15 Dash (DASH) – MC $986M. TV $110.35

17 NEO (NEO) – MC $809M. TV $11.47

26 Zcash (ZEC) – MC $495M. TV 70.52

All figures were taken as at 23rd July 2019 (source Coinmarketcap).

TOP 11 CRYPTOS (INC BTC) 2021

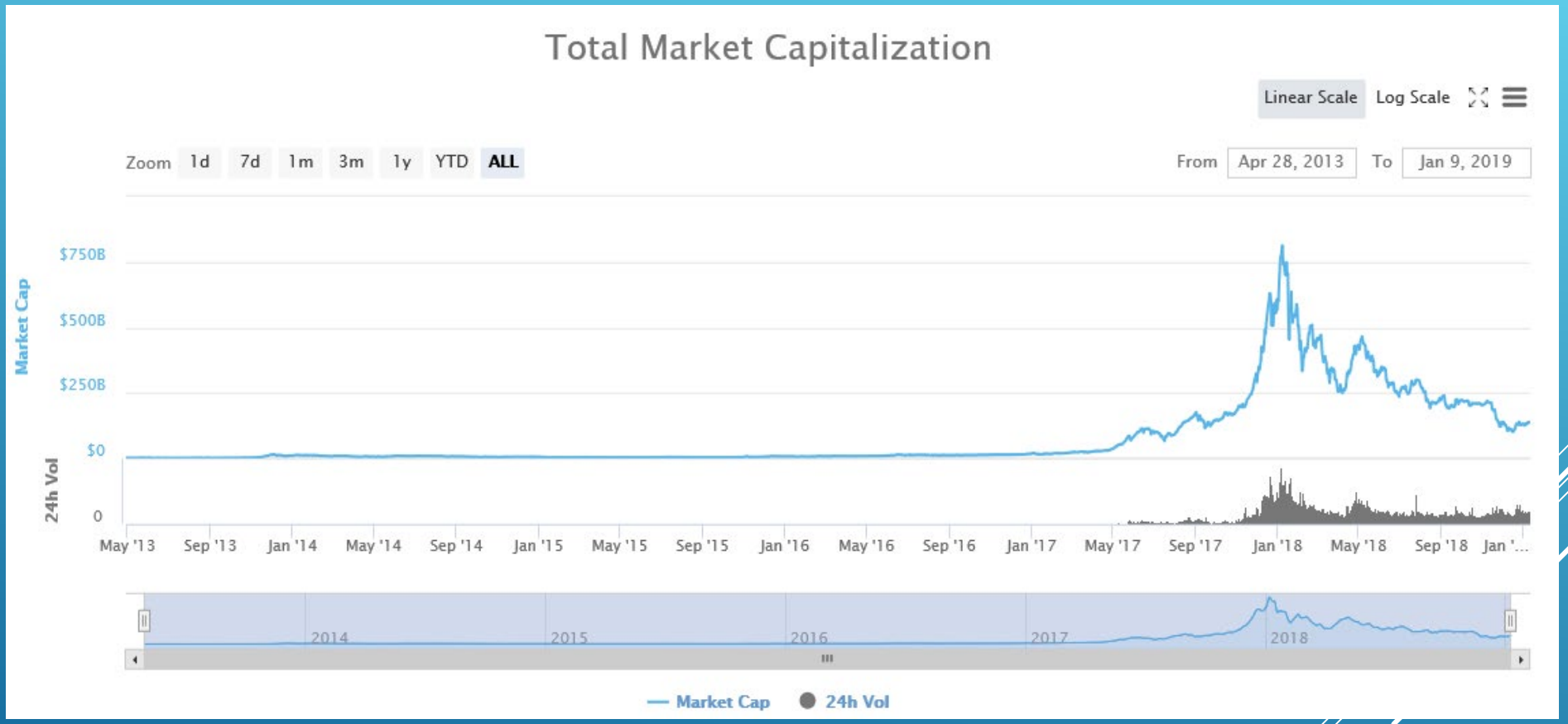
1	Bitcoin BTC Buy	$46,183.08	-0.32%	-7.35%	$867,579,212,637	$34,454,650,624 747,085 BTC	18,811,837 BTC	
2	Ethereum ETH Buy	$3,395.64	-2.59%	-14.21%	$397,524,720,363	$20,621,358,813 6,093,422 ETH	117,464,896 ETH	
3	Cardano ADA	$2.48	-4.22%	-16.61%	$79,351,881,398	$5,226,549,135 2,109,395,382 ADA	32,025,814,324 ADA	
4	Binance Coin BNB Buy	$414.86	-0.39%	-15.00%	$69,583,638,312	$2,372,647,496 5,733,099 BNB	168,137,036 BNB	
5	Tether USDT Buy	$1.00	-0.02%	-0.01%	$68,361,309,812	$91,325,502,818 91,309,876,815 USDT	68,349,613,035 USDT	
6	Solana SOL	$183.06	-12.17%	+32.54%	$53,401,106,096	$9,037,689,759 49,599,475 SOL	293,069,012 SOL	
7	XRP XRP	$1.09	-2.41%	-14.31%	$50,584,391,574	$7,616,561,279 7,014,409,898 XRP	46,585,282,244 XRP	
8	Dogecoin DOGE	$0.2484	-2.67%	-16.35%	$32,541,224,383	$1,823,259,110 7,352,601,560 DOGE	131,228,005,837 DOGE	
9	Polkadot DOT	$31.17	+6.69%	-4.32%	$30,630,712,096	$3,740,879,989 120,611,486 DOT	987,579,315 DOT	
10	USD Coin USDC	$1.00	-0.01%	+0.03%	$28,951,187,988	$3,194,266,807 3,193,812,088 USDC	28,947,066,645 USDC	
11	Terra LUNA	$38.31	+27.99%	+15.81%	$15,294,001,894	$2,142,066,330 56,637,352 LUNA	404,381,397 LUNA	

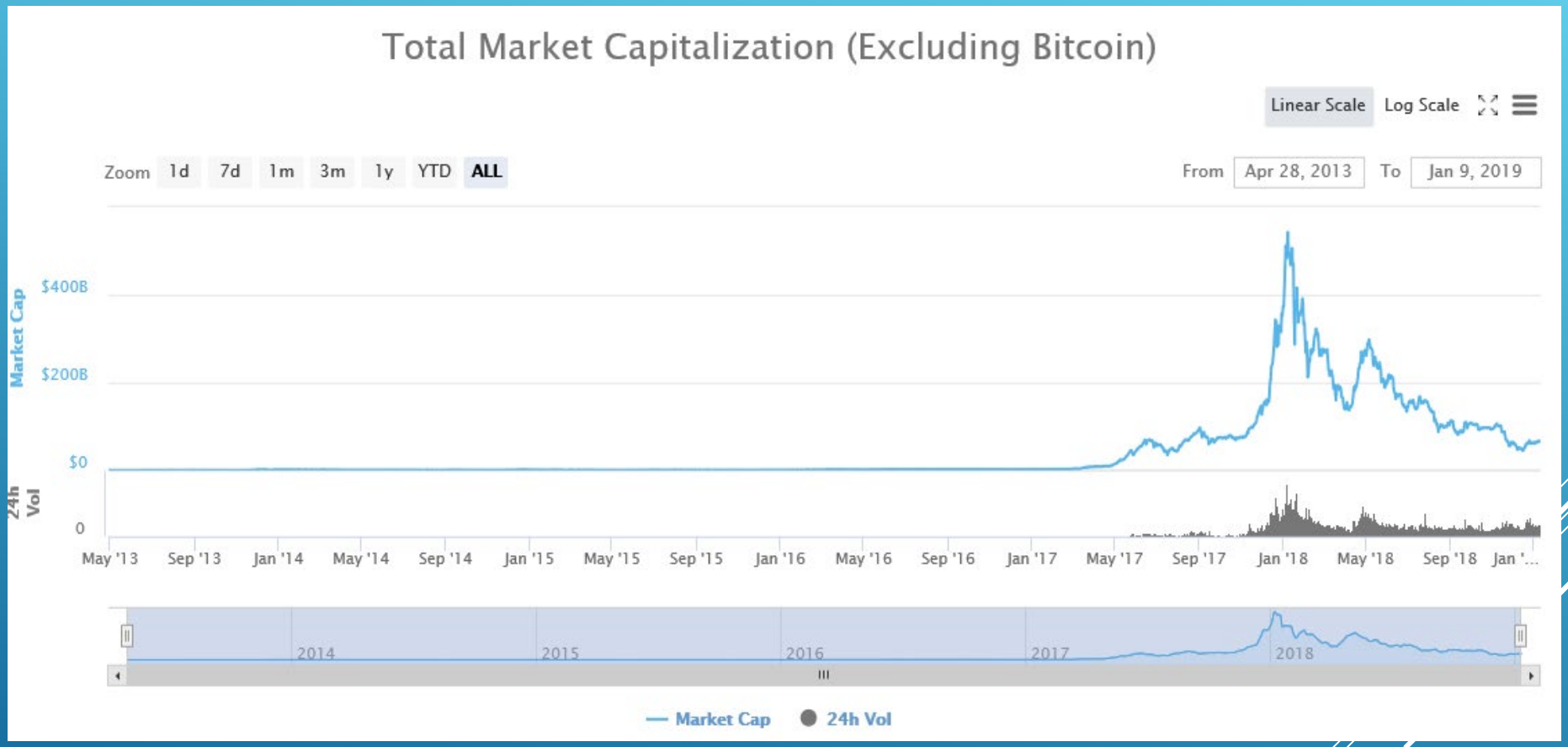
TUESDAY 20 NOVEMBER 2018 13:28
THE INDEPENDENT

- Cryptocurrency markets have lost more than $60 billion in value in less than a week, following a price crash that has caused bitcoin, ethereum and ripple to hit their lowest levels since 2017.
- The price falls appear even more dramatic given the remarkable period of stability that preceded them, which had prompted some analysts to warn that the lack of any major market movement since early September would likely be the "calm before the storm."
- Speculation around why the cryptocurrency collapse has happened focusses not on bitcoin but its spin-off, bitcoin cash
- On 15 November, the rival cryptocurrency experienced something called a hard fork, whereby a brand new cryptocurrency was created. This led to uncertainty in the market and a major sell-off of bitcoin cash.
- With a market cap of around $4 billion, bitcoin cash is the world's fourth most valuable cryptocurrency, however more than half of its value has been wiped off since last week's split.
- It is not clear if or when the crypto market will level out, with many of the price predictions from earlier this year now looking improbably optimistic. (Fortune 19-11-2018 – 3 reasons for collapse) & (Smartereum – Real reason behind Btc price crash)

EFFECT OF 2018 COLLAPSE

- January 2018 – Market Capitalisation of Cryptocurrencies was $831 BILLION
- November 2018 - Market Capitalisation of Cryptocurrencies was $186 BILLION
- December 2018 - Bitcoin price below $3,300 - January 2018 peak of $19,800 – lowest since August 2017
- Ethereum – 2ND Largest coin by Market Cap suffered heavy losses
- Heavy value loss also for Ripple, Bitcoin cash, EOS
- Now only 3 Coins with a market cap of over $10 BILLION – Bitcoin, Ethereum and Ripple
- Previously there has been over 10 coins in this category
- Bitcoins percentage of Total Crypto Market Cap – up to 57.8% (it was 85% in March 2017 before the rise of other Altcoins lowered it). Bitcoin regaining dominance of market.


Total Market Capitalization
Linear Scale
Log Scale
Zoom
1d
7d
1m
3m
1y
YTD
ALL
From
Apr 28, 2013
To
Jan 9, 2019
Market Cap
$750B
$500B
$250B
$0
24h Vol
0
May '13
Sep '13
Jan '14
May '14
Sep '14
Jan '15
May '15
Sep '15
Jan '16
May '16
Sep '16
Jan '17
May '17
Sep '17
Jan '18
May '18
Sep '18
2014
2015
2016
2017
2018
Market Cap
24h Vol


Total Market Capitalization (Excluding Bitcoin)
Linear Scale
Log Scale
Zoom
1d
7d
1m
3m
1y
YTD
ALL
From
Apr 28, 2013
To
Jan 9, 2019
Market Cap
$400B
$200B
$0
24h Vol
0
May '13
Sep '13
Jan '14
May '14
Sep '14
Jan '15
May '15
Sep '15
Jan '16
May '16
Sep '16
Jan '17
May '17
Sep '17
Jan '18
May '18
Sep '18
2014
2015
2016
2017
2018
Market Cap
24h Vol

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$70,734,832,022	$4,048.45	17,472,062	$5,303,174,959	-0.40%	-0.31%	4.91%
2	Ethereum	ETH	$15,836,609,909	$151.87	104,278,709	$2,356,763,605	-0.61%	-0.28%	1.73%
3	XRP	XRP	$15,059,764,142	$0.369165	40,794,121,066 *	$490,006,613	-0.42%	1.22%	0.73%
4	Bitcoin Cash	BCH	$2,828,608,307	$161.11	17,556,800	$166,020,111	-0.41%	-0.25%	-2.25%
5	EOS	EOS	$2,555,435,551	$2.82	906,245,118 *	$668,840,725	-0.95%	0.06%	3.28%
6	Litecoin	LTC	$2,370,372,301	$39.55	59,940,425	$595,789,795	-0.83%	-0.69%	21.65%
7	Stellar	XLM	$2,369,035,853	$0.123623	19,163,348,774 *	$97,774,664	-0.38%	-0.01%	6.68%
8	Tether	USDT	$1,923,757,109	$1.02	1,885,043,152 *	$3,717,083,397	0.08%	0.44%	0.38%
9	TRON	TRX	$1,841,266,791	$0.027628	66,644,003,916	$214,010,015	0.23%	5.75%	40.00%
10	Bitcoin SV	BSV	$1,539,795,056	$87.71	17,555,836	$50,610,600	-0.28%	-0.35%	-4.54%

11	Cardano	ADA	$1,330,275,367	$0.051308	25,927,070,538 *	$44,480,119	-0.19%	4.15%	18.96%	•••
12	IOTA	MIOTA	$1,032,203,599	$0.371359	2,779,530,283 *	$7,431,926	-0.33%	0.20%	-1.57%	•••
13	Monero	XMR	$904,077,079	$54.14	16,697,487	$17,504,329	-0.49%	0.93%	8.58%	•••
14	Binance Coin	BNB	$892,858,218	$6.83	130,799,308 *	$73,330,976	-0.83%	1.54%	13.67%	•••
15	Dash	DASH	$708,068,913	$82.74	8,558,254	$100,676,379	-0.60%	-0.71%	0.93%	•••
16	NEO	NEO	$619,373,441	$9.53	65,000,000 *	$197,658,890	-2.36%	4.50%	20.20%	•••
17	NEM	XEM	$581,725,559	$0.064636	8,999,999,999 *	$13,061,359	-0.45%	0.06%	-2.18%	•••
18	Ethereum Classic	ETC	$542,590,398	$5.05	107,390,231	$121,149,152	-0.72%	-0.29%	-5.21%	•••
19	Maker	MKR	$350,301,182	$481.03	728,228 *	$6,938,901,624	0.01%	-2.54%	-0.85%	•••
20	Zcash	ZEC	$344,671,718	$61.17	5,634,219	$124,420,170	-0.14%	0.44%	1.72%	•••
21	USD Coin	USDC	$329,107,511	$1.01	326,312,885 *	$23,767,765	0.19%	-0.35%	-0.55%	•••
22	Tezos	XTZ	$295,046,852	$0.485683	607,489,041 *	$3,323,150	-0.04%	-0.12%	0.52%	•••
23	Waves	WAVES	$292,019,230	$2.92	100,000,000 *	$15,020,951	-0.24%	-2.44%	-6.21%	•••
24	Dogecoin	DOGE	$269,822,204	$0.002291	117,751,214,005	$19,625,227	0.79%	0.10%	-4.28%	•••

THE THREAT THEN 2018

- Europol Report 2017 Virtual Currencies Money Laundering Typologies
- Daily transaction volume of VCs already exceeds that of major MSBs (Paypal and Western Union) [1]
- Regulatory framework does not classify VCs in any category of traditional fiat currency or legal tender ….
- "an unregulated payment instrument with manifold opportunities for exploitation for money laundering purposes"
- What makes them so attractive to criminals? [2]
- "they represent a powerful tool for criminals to covert, move and store illicit funds, out of the reach of LEAs"
- NCA Report June 2018 – updated threat assessment from February 2017 increase in threat from use of CCs

KNOWN USES OF CRYPTOASSETS

- Money Laundering
- Extortion – ransomware, DDOS
- Blackmail
- Kidnapping
- Fraud
- Drugs
- Terrorist Financing
- State evasion of sanctions
- Cryptomining or Cryptojacking - Indian government websites – September 2018
- Initial Coin Offerings

STATE OF PLAY 2018

- Share of BTC transactions sent to the Darknet markets has declined from 30% in 2012 to less than 1% in 2017 (absolute value increased $660M in 2017 from $57M in 2012)
- Reasons – (1) LEAs have closed the largest Darknet markets, (2) BTC use has evolved – more seen as a financial asset, (3) Growing use of other CCs.
- Darknet Markets – Closed Silk Road, Alphabay, Hansa Market and Russian Anonymous Marketplace (RAMP)
- Silk Road accounted for 99% of all Darknet market activity (October 2013)
- AlphaBay, Hansa Market and RAMP accounted for circa 87% (July 2017)
- Effects – BTC came into mainstream due to reducing links to OC
- BTC had a 14x increase in value in 2017 – consequence less useful as exchange means for criminal use.
- Rapid growth BTC as asset – 2017 tens of billions $ sent to exchanges as compared to $660M to Darknet

THE RISE OF OTHER CRYPTOASSETS – ALTCOINS 2018

- Other CCs taking over Darknet markets – Monero, Zcash, Dash.
- Benefits – lower transactions fees than BTC & greater anonymity
- Monero network increase transactions by 230% in 2017
- Acceptance has increased (Tochka & Aero added Monero 2017, Libertas only accepts Monero)

GREG KELLY

HMRC Fraud Investigation Service
Senior Investigation Officer
Money Laundering Cryptoasset SME
Illicit Finance Strategy
Economic Crime Division

INVESTIGATION PRACTICALITIES PART 1

- CHALLENGES FOR LEAs
- WHAT TO LOOK FOR
- SEIZING CRYPTOASSETS
- LEGISLATION or POWERS

Money Laundering

- Rob Wainwright – Director of Europol stated that 3% – 4% of the illicit funds being laundered in Europe is being done so using CCs. That equate to £3B to £4B per annum.
- He also added "It's growing quite quickly and we are quite concerned".
- Most exchanges require ID documents and undertake CDD – NOT ALL
- Use legitimate exchanges and circumvent verification process – fake IDs
- Different payment methods offered to buy or sell CCs – bank transfers, credit or debit cards, MSB, PayPal, bank cheques and CASH
- Localbitcoin.com and BTC events advertised ie meet ups in larger cities
- 247exchange.com and Cex.io – BTCs can be purchased with prepaid debit and credit cards without need to provide formal ID documents
- Some exchanges upgraded their CDD – Skype verification calls or self-generated images holding their ID and papers with a random text written on it
- 2017 Investigations into ML via abuse of exchanges or complicity

Challenges facing Law Enforcement

- Identification of use – how do you find out that they using CCs to launder funds, purchase goods, etc?
- Once you know what power do you have to seize it? Legislation
- What tools do you have to seize it? Physical act of seizure/transfer
- How do staff recognise the signs of it?
- Once you have it how do you store it? Legislation to retain. Physical storage and the security concerns surrounding it. 1
- Realisation?
- How do you conduct your investigation?
- Tracing its usage on Blockchain. Track and Trace open source tools. Use requires expertise and a certain amount of knowledge.
- Use of tumblers/mixers to obfuscate path by criminals. Private companies offer user friendly alternatives.
- Software - availability of access to LEAs – limited number of licences (UK)

Benefits to a Criminal

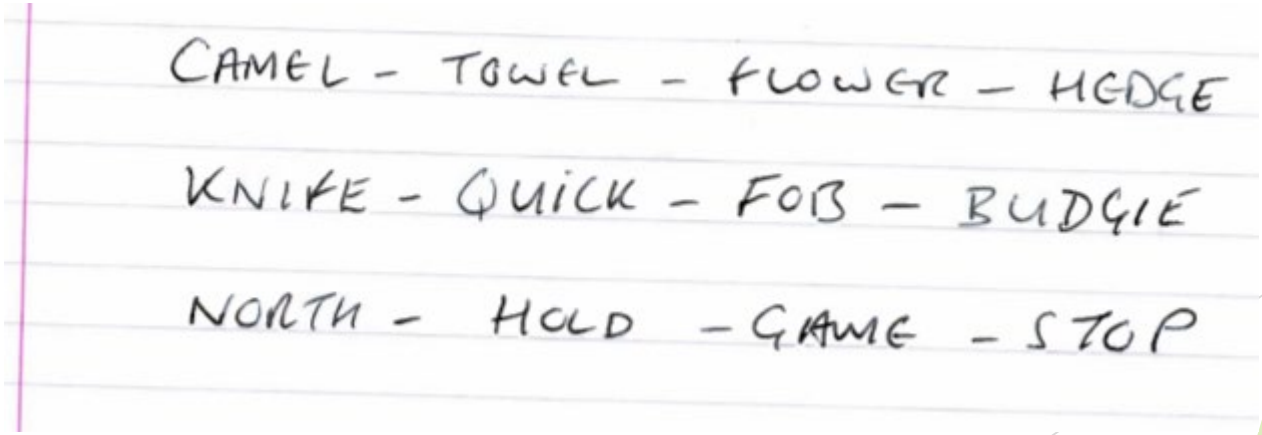
- Lack of Regulations governing use - decentralised
- Pseudo-anonymous nature of CCs
- LEAs lack of experience in dealing with CCs
- Availability of additional software – mixers/tumblers (1)
- Exchanges – lack of robust "proper" KYC
- Localbitcoins.com – legitimate website. Just enter postcode. (2)
- No reporting mechanisms in place for suspicious transactions
- Bitcoin ATMs – No regulation on BTC ATMs in the UK. Ideal opportunity to launder and transfer proceeds of crime. (3)
- Ease to carry and store – phone, memory stick – Trezor, Ledger and KeepKey
- Easy to move internationally outside of supervision click of a button or held on a memory stick
- Accounts cannot be frozen if identified like traditional banks

What to look for?

- A Bitcoin Address is an alpha-numeric string of between 26 to 35 characters (usually 33). Begins with either 1 or 3
- It can also be visualised as a QR code. Newer BTC addresses might start “bc1”
- Private Keys are either 51 or 52 alpha-numeric characters which usually begin with 5, L or K.
- If you control the **Private Key** then you control the **Bitcoin**

What to look for?

- A Recovery Seed is what would appear to be a random set of words 12, 18 or 24 in length.
- It is a readable interpretation of the private keys
- This can be used to restore a wallet without having access to the original wallet or hardware device itself.
- Once accessed the contents can be transferred to a wallet controlled by the LEA
- R-I-S-K – anyone who has sight of the recovery seed can recover the bitcoins and transfer them anywhere and at any point in time (1)



Syndicate Exercise

- You or a member of your staff are out on a job and you come across a Recovery Phrase
- What would you do?
- How would you deal with this in your jurisdiction?
- Legality - powers
- Physical actions
- Storage
- Security

UK Powers – POCA 2002 S47

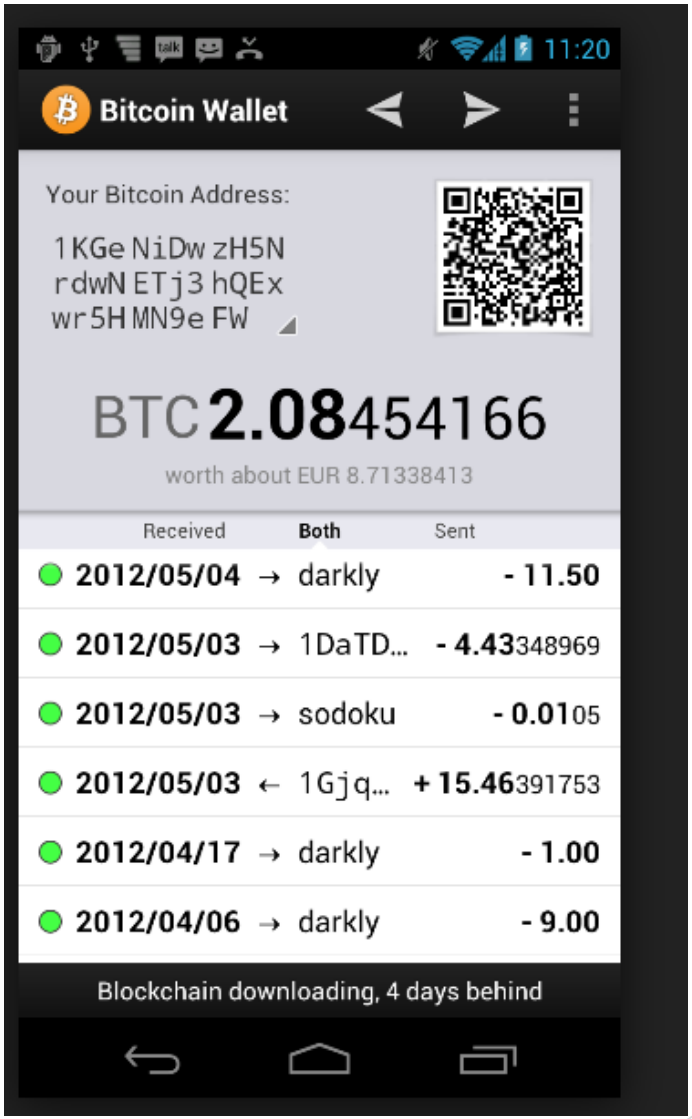
- This allows for seizure and detention when there are reasonable grounds for suspecting that realisable property may be unavailable for any future confiscation
- If a seizure is expected or planned as part of an operation then prior authorisation should be sought from a Magistrates court
- If there is an urgent need to use S47 then an Inspector grade can authorise it
- S47 is only activated/required at the point that the CC is transferred into an LEA wallet
- Once seized the LEA applies for detention at Magistrates court – usually 3 months
- Once the initial 3 months has been granted LEAs apply for a S41 POCA Restraint Order
- As part of the order LEAs have been applying for a realisation order as part of the process
- UK LEAs have been using a Dutch company – Bitonic for realisation of CCS back into FIAT currency

Wallets

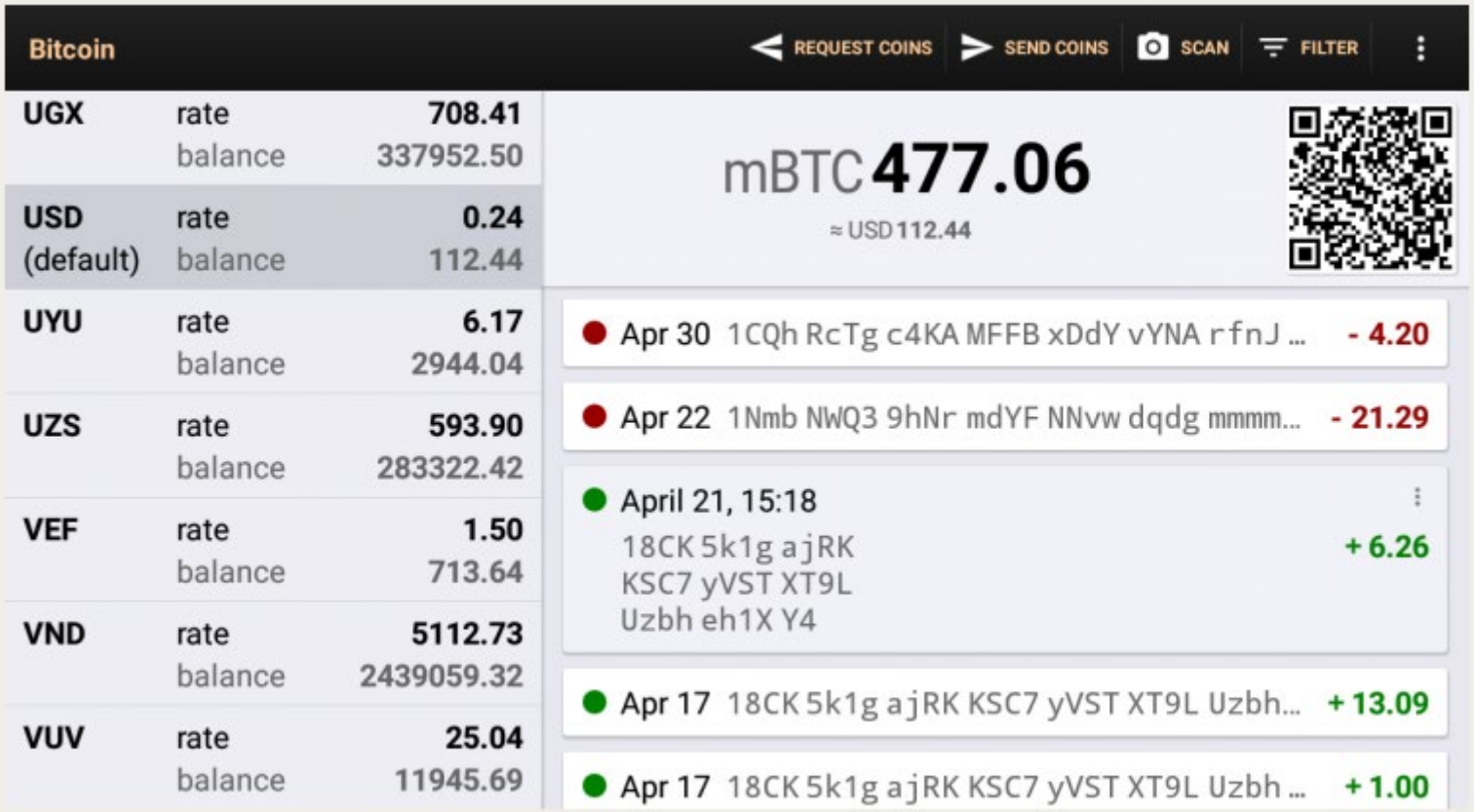
- **Web based wallet-** allow you to send, receive, and store bitcoin all through your web browser.
- **Desktop wallet**- wallet software directly on your computer
- **Mobile wallet-** simply designed for a mobile device
- **Hardware**- specialized type of device designed specifically to store bitcoins
- **Paper**- written record of private keys, addresses

OFFICIAL

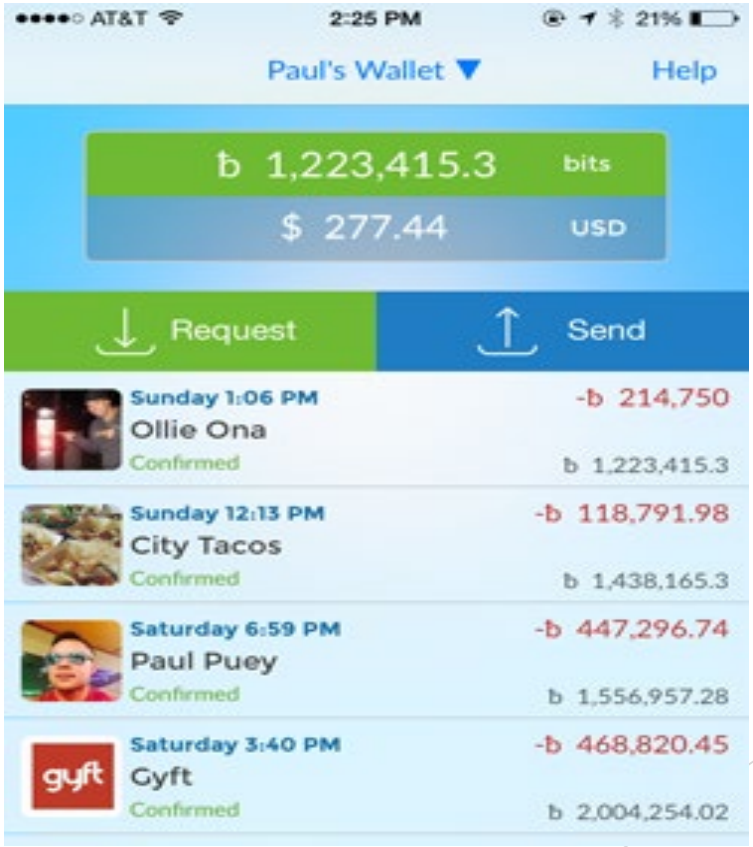
Bitcoin Wallets



Bitcoin Wallet



BITCOIN WALLET	
Address	Private Key (usually hidden from screen)
1KrieA3KyYVrLJbSynkML9rriBLZpkPvDR	5J7ZWKWJE1fMSjQSTyeBqD4cxickKKA7xFdYHZDeXVbmoPBLrey
1KKGgesMtkWW52SEyd88kBkSijhVps7nJJ	5JwGTvMJumhMtxNBSj5QdYZVSck5W8PqAC5mtEUnRA1xHpL9g5x
14wKRvadKMq6Lthg9HAic5iebKWGSY2w75	5JphsyRvz3Goves7GVzntJ4bVpTWnmExXsjK3fHe6zhRqrgZoDT



Bitcoin Wallet

- Bitcoin Wallet has no central service and provides zero trust
- Decentralized and Peer to Peer
- No Registration, No web service, No Cloud needed.
- Displays Bitcoins held in various formats
- Conversion to and from FIAT currencies
- Address book for regularly used addresses
- When offline you can still transact via Bluetooth
- System notification for received coins
- Sweeping of paper wallets
- Sending and receiving of Btc via NFC, QR codes or Bitcoin URLs

OFFICIAL

Paper Wallets – Cold Storage

via bitaddress.org

What is printed on the paper wallet are the private and public keys, usually in QR form, with the latter also serving as the address. You could just copy and paste the keys onto a text document and print that out (erasing the copy on the computer afterwards). Or you could use one of the free web services that generate the printable wallet for you. The key generation is usually done in your browser, so they are never transmitted on the internet. To be safe, you should clear your browser after printing. And never store an image of the paper wallet on your computer or phone.

Some paper wallet services have a nifty design that you can cut, fold and seal, making them a lightweight and relatively secure form of storing bitcoin offline. You send your bitcoin to the public address displayed on the wallet, and then store it in a secure place.

via bitcoinpaperwallet.com

Hardware Storage

- Popular Hardware wallets – Trezor, Ledger and Keepkey – can be used to store specific Cryptoassets
- Bitcoin, Bitcoin Cash, Ethereum, Litecoin, Dogecoin, Dash, Bitcoin Gold and others
- Extra layer of security – password, seeds
- Exchange between assets directly on the device using Shapeshift
- Virus and malware proof
- Available on PC, Mac, Linux and Android
- Supported by Electrum and Mycelium

Trezor

Ledger

Keepkey


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

FOUNDATION

FOUNDATION


Passport
Sign with QR Code
Sign with MicroSD
Verify Address
Enter Passphrase
Settings
Shutdown
BACK
SELECT

Seizure of Cryptoassets

- How can you seize a Cryptoasset?
- Legal basis – what laws exist to allow you to do this?
- Practical basis – how are you going to physically take control of it?
- R-I-S-K
- Movement of asset from criminal wallet to government controlled wallet
- Temptation/Corruption – how do you lessen the risks? Support staff?
- Seizure on the ground in real time – US and Australia strategies
- UK based strategy – remote seizure of assets
- Technology available
- Supporting infrastructure for technology
- Storage concerns

Challenges to an Investigating LEA

- Cannot trace transactions using standard ML tools and methods
- Banking data of little use – cash in, cash out points only
- Insufficient tools available for the investigator
- Targets often use encrypted messages to convey information
- Targets are un-cooperative – no passwords – how do you access device?
- How do you go about attributing a specific wallet to an individual?
- How do go about obtaining information from cryptocurrency exchanges when most of them are overseas? Cloud based systems – where is there legal entity based?
- Knowing who to go to – who has the knowledge? Expertise?
- Getting an expert witness to go to court to explain this to the judge and jury
- Legislation is not in place to allow you to pursue various avenues

Conducting an Investigation

- Tracing transactions on Blockchain
- OCGs use TOR network or other to mask IP addresses. Use of mixers.
- Dark Wallets seek to anonymise BTC – combines random contemporaneous transaction & encrypts recipient's information so it does not appear on Blockchain
- Hardware & E-wallets – plausible deniability mechanisms added – create hidden wallets attached to visible ones
- Customised "white-label" services – supply software and infrastructure for those who want to create their own CC exchanger.
- www.Blockchain.com – tells you how many BTCs are held under an address. www.blockchair.com – allows you to search for transactions across 17 different blockchains
- www.WalletExplorer.com – shows if BTC were used on Darkweb &/or originate from a mixer.
- Private companies – Chainanalysis and Elliptic provide training and software packages. Also offer their own analysts who produce court ready reports
- Tracing any CC other than BTC is very difficult. Lessens with Mixers. Monero and Zcash more security features to obfuscate Blockchain tracing

Available Investigation Tools/Assistance

- FIOD devised a wallet identifier – available on Europol website – enter mnemonic phrase – it will tell you
- Luxemborg FIU – have the power to freeze crypto wallets held with exchanges
- www.weseizebicoins.com and www.weseizevirtualcurrencies.com both available on Europol platform
- Graphsense Github – open source cryptocurrency analytical platform.
- Open Source tool “Titanium”
- Interpol also have tools and library available

Greg Kelly

HMRC Fraud Investigation Service
Money Laundering Cryptoasset SME
Economic Crime Operations

Investigation Practicalities PART 2

- OTCs
- DEX
- MIXERS
- DARK WALLETS
- GLOSSARY TERMS

Bitcoin Traders – Peer 2 Peer

- The BUYER
- Offers services via internet through supply & demand sites
- Does not ascertain identity of seller
- Does not display his own name
- Pays in **CASH**
- Charges an unusually high commission percentage (7 to 15% not 0.3%)
- The transaction takes place in public place – less risk to buyer
- There is no plausible legal or economic reason for this exchange type
- The sheer amount of CCs purchased is implausible for personal use
- The Buyer is not registered with the authorities for his exchange facilities
- The Buyer and/or Seller make use of a Mixer during the sale transaction of the CCs

Peer to Peer Exchanges - Recap

- Peer-to-peer (P2P) exchanges differ from regular exchanges – no set prices for the currencies -matches buyers with sellers who can set their own prices and payment forms.
- Attractions for criminals looking to launder their currency – (1) instant access to cryptocurrencies without any rigorous customer due diligence checks. (CDD can be overcome easily using counterfeit or forged ID documents), (2) – They allow the transfer of ownership of a cryptocurrency wallet without the transaction appearing on the blockchain, as the wallet is simply handed over to the new owner in exchange for cash (or some other commodity).
- The use of peer-to-peer exchangers by traditional laundering groups has already been observed.
- The Spanish Guardia Civil observed an OCG using the LocalBitcoins platform to launder and quickly transfer substantial value from Europe back to Columbia. (They also used traditional laundering methods alongside this).
- In the UK, Ryan Kennedy used LocalBitcoins to sell some of the more than 3,700 Bitcoins that he had stolen from customers who used the popular MintPal exchange that he co-owned

Buy and sell bitcoins near you

Instant. Secure. Private.

Trade bitcoins in 16375 cities and 248 countries including United Kingdom.

Sign up free

QUICK BUY | QUICK SELL

Amount | GBP | United Kingdom | All online offers | Search

Buy bitcoins online in United Kingdom

Seller	Payment method	Price / BTC	Limits	
vaidelis (100+; 100%)	National bank transfer: United Kingdom	5,057.49 GBP	200 - 1,378 GBP	Buy
fanbitcoin10 (1000+; 100%)	National bank transfer: United Kingdom	5,091.83 GBP	300 - 1,000 GBP	Buy
Vee-man (500+; 100%)	National bank transfer: United Kingdom	5,091.00 GBP	50 - 1,000 GBP	Buy
softgamers (3000+; 100%)	National bank transfer: United Kingdom	5,101.64 GBP	100 - 1,000 GBP	Buy
Nicogranto (22; 100%)	National bank transfer: United Kingdom	5,100.00 GBP	100 - 306 GBP	Buy
BitGuruq (100+; 100%)	National bank transfer: United Kingdom	5,122.59 GBP	100 - 2,561 GBP	Buy

Sell bitcoins online in United Kingdom

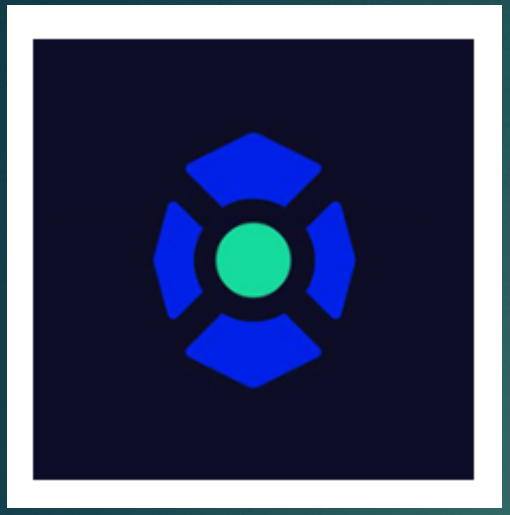
Buyer	Payment method	Price / BTC	Limits	
london1103 (1000+; 100%)	Cash deposit: Any Bank/Branch/No Cancelletion 👍	5,028.06 GBP	200 - 8,000 GBP	Sell
seraphicus (100+; 100%)	Cash deposit: Halifax, Lloyds, TSB, HSBC ☺ FAST DEPOSIT ☺ 👍	5,019.72 GBP	100 - 5,178 GBP	Sell
nersi55 (100+; 100%)	Cash deposit: ✕Lloyds,HSBC,Halifax,TSB,Metro✕ ⋆ Fast Deposit ⋆ 👍	5,010.52 GBP	400 - 7,000 GBP	Sell
Mr.JonesUK (1000+; 99%)	Cash deposit: HSBC, Halifax, TSB, Llyods - FAST DEPOSIT 👍	4,998.62 GBP	100 - 6,340 GBP	Sell
CharaCoins (1000+; 100%)	Cash deposit: Lloyds I HSBC I Halifax I Metro I Fast and Trusted 👍	4,985.96 GBP	1,000 - 8,000 GBP	Sell
LakeHouse (1000+; 100%)	Cash deposit: HSBC, Lloyds, TSB, Halifax, Metro - QUICK PAYMENT 👍	4,954.48 GBP	100 - 32,649 GBP	Sell

Buy bitcoins with cash near Southend, United Kingdom

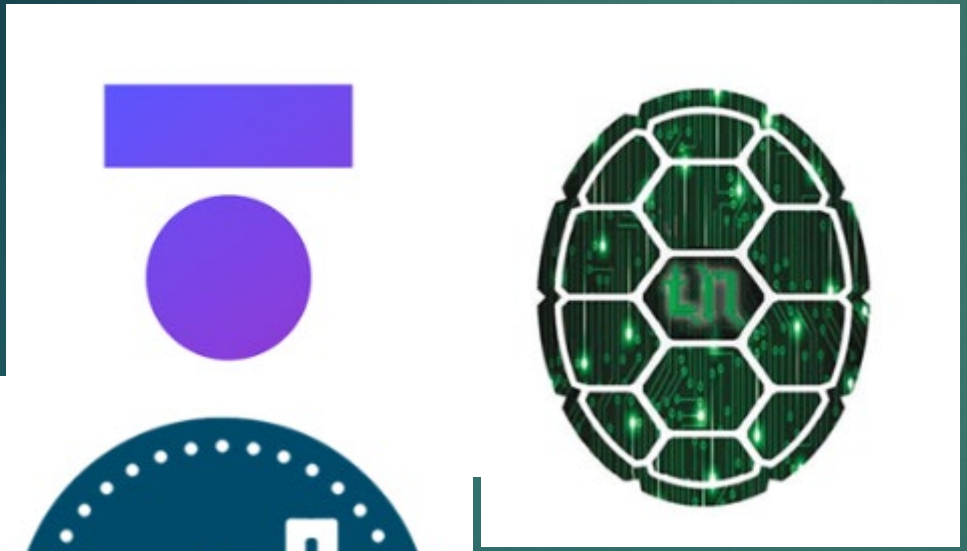
Seller	Distance	Location	Price/BTC	Limits	
Quick.Bit_Sam (100+; 100%)	27.5 km	Essex, UK	5,003.53 GBP	1,000 - 100,000 GBP	Buy
B.I.G (1000+; 100%)	27.5 km	Essex, UK	5,297.85 GBP	5,000 - 500,000 GBP	Buy
CoinSense.Chris (100+; 98%)	27.5 km	Essex, UK	4,512.99 GBP	1,000 - 100,000 GBP	Buy
CoinSense.Chris (100+; 98%)	27.6 km	Chelmsford, UK	4,512.99 GBP	1,000 - 100,000 GBP	Buy
m4ttyd (3000+; 98%)	28.6 km	Middleton Hall La, Brentwood CM15 8EQ, UK	5,126.17 GBP	2,500 - 500,000 GBP	Buy

Decentralised Exchanges (DEX)

- A Crypto-Asset exchange which facilitates peer to peer exchanges of crypto-assets via an automated process
- Customers do not have to transfer their assets to the exchange
- Reduced risk of hacking
- Attractive as user does not have to trust security or honesty of the site as they retain control of their crypto-assets
- More anonymous as they do not implement KYC – unless use of a FIAT currency bank transfer is involved. Seller will know buyer identity
- Hosting of DE is distributed through nodes involved so no risk of downtime
- Can have some parts under a central control - IDEX
- Due to lack of KYC and nature of crypto-asset exchanges there is a risk to users if they are hacked for private keys or passwords
- They are not easy to use
- They have low liquidity
- Bisq – requires users to be on-line in order to proceed with trade and require users to perform certain actions to confirm transaction conducted




REMITANO




TRXMarket

DEX

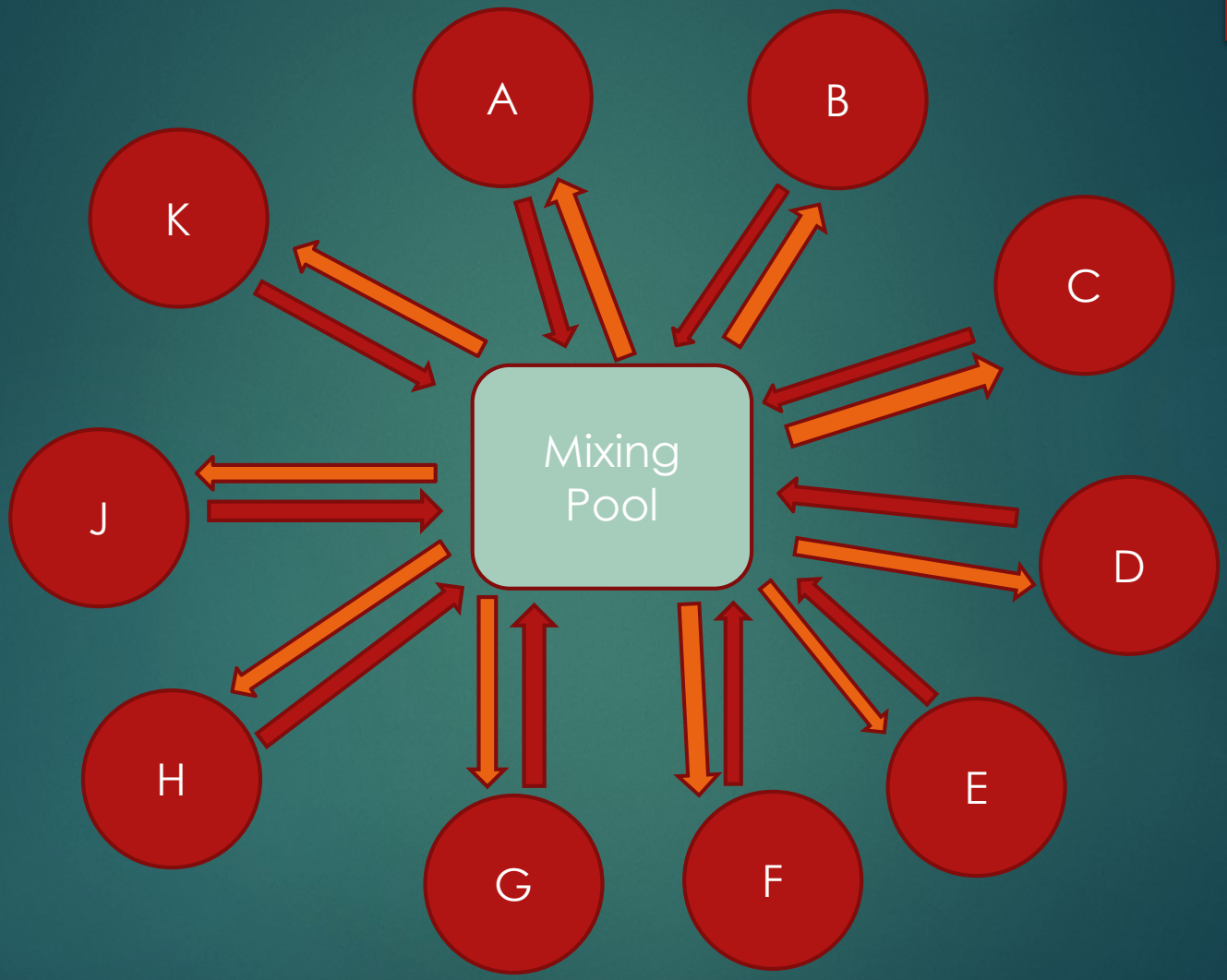
- EtherMium – a multi crypto-asset exchange platform
- Remitano – P2P exchange Bitcoin & Ethereum. Seychelles based
- Bisq – One of the largest multi-crypto DEX. Allow crypto to fiat, and vice versa
- Token Store – exchange for Ethereum based tokens
- Turtle Decentralized – allows for trade of tokens created on Turtle network
- TRX Market – First DEX based on Tron network. All trades are carried out in TRX smart contracts and transaction records stored in Blockchains – open and transparent
- IDEX – exchange for Ethereum based tokens. Has it's own token – Aurora.

OFFICIAL

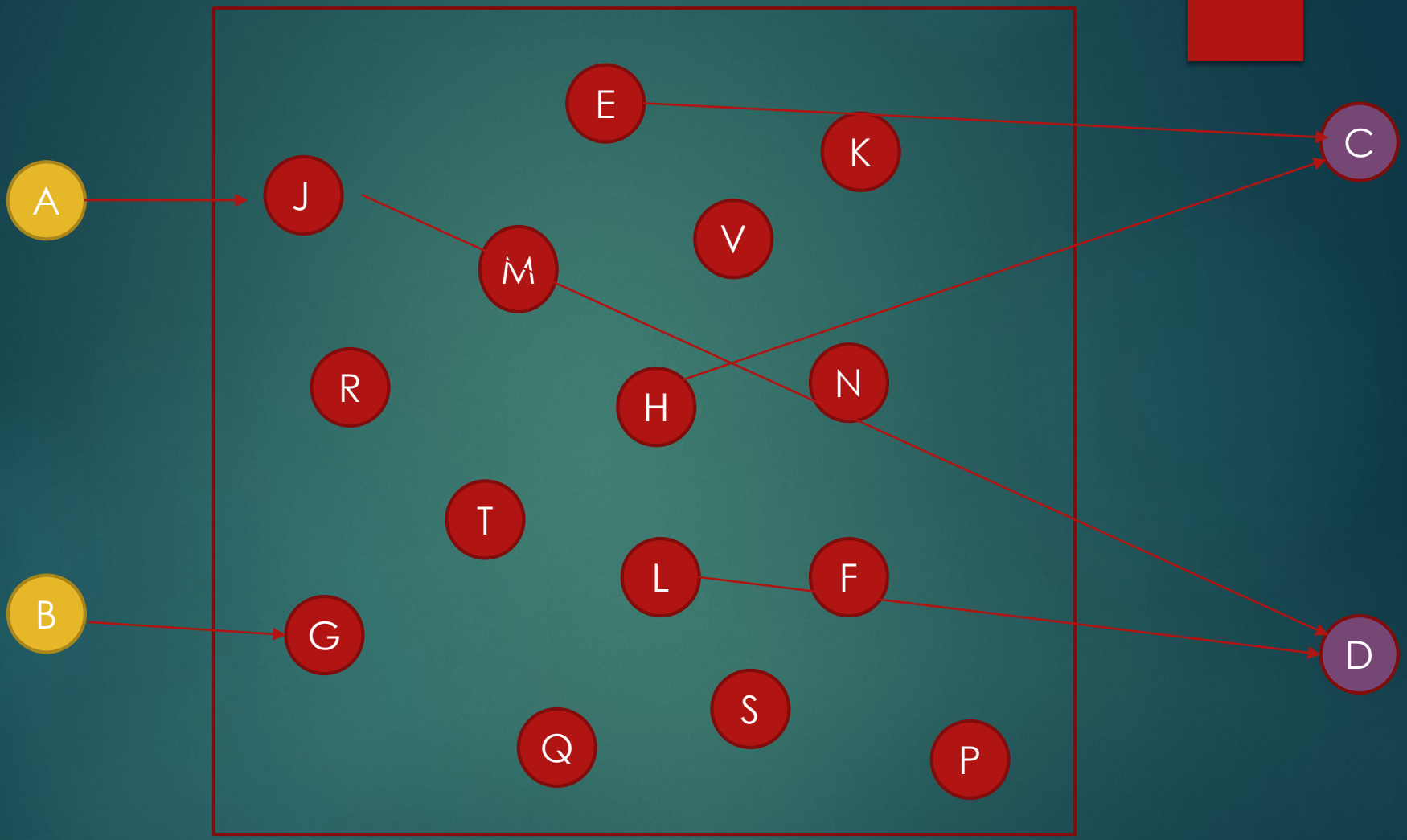
The Use of Flippers

- Differ from actual Exchanges as they only covert one Crypto into another Crypto with no FIAT currency being involved
- Mainly used to change bitcoin into more privacy centric currency ie: Monero or Zcash
- SHAPESHIFT – popular with launderers as service can be used without signing up for an account
- CHANGELLY or CHANGENOW
- Wannacry participants used Shapeshift & Changelly to exchange Bitcoins
- August 2017 – Wannacry attempted to exchange Bitcoin for Monero using Shapeshift – who blacklisted their wallets. Too well known and amount too large.
- January 2018 – theft of $500 MILLION worth of NEM from CoinCheck. Shapeshift blacklisted wallets.

How Mixers work



OFFICIAL

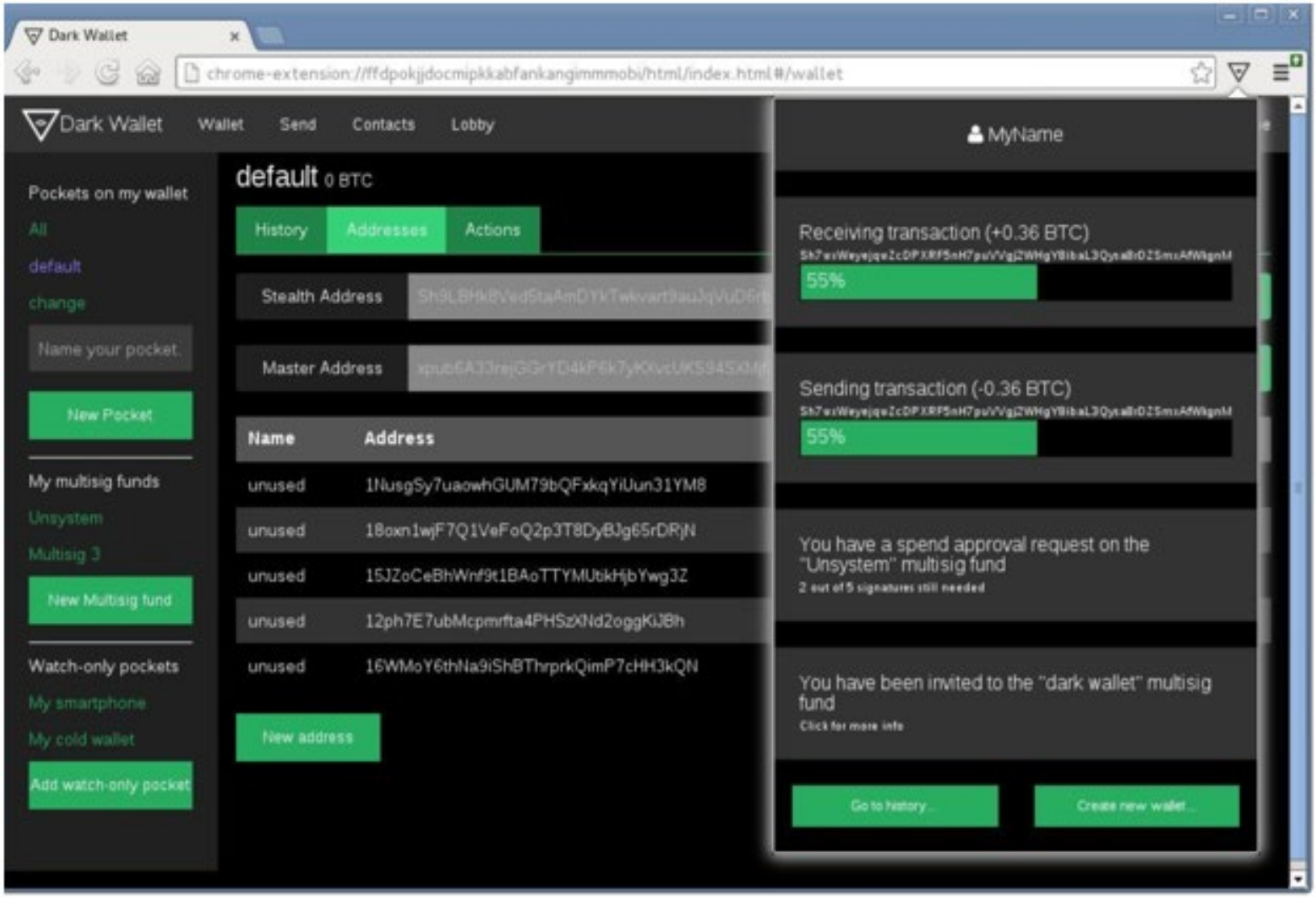

E
K
C
A
J
V
M
R
H
N
T
L
F
B
G
D
S
Q
P

Mixers & Tumblers

- These are services that increase the anonymity of cryptocurrencies
- Fee is paid – mix tainted Crypto with the Crypto of service provider or other users of the mixing service provider
- Best if there is a high amount of users – otherwise possibly still traceable
- Mixes illegally obtained funds with "clean" funds
- Some wallets can include built-in mixing services – ie: DarkWallet
- Some Darknet marketplaces also contain a built-in mixer ie: Alphabay
- Chainanalysis estimated that in first half 2016 approx. 160,000 (or2%) of more than 6 Million Bitcoin sent worldwide involved mixing.
- Estimated that up to 10% of daily value of Bitcoin transactions could involve mixing.
- Drawbacks – users becoming sceptical – perceived unreliability and insecurity

Dark Wallets

- It is a browser app for Bitcoin payments that uses both encryption and CoinJoin technology
- CoinJoin mixes multiple transactions, selected at random, as one transfer of funds and conceals the original payers
- Concept is users can route transactions through a shared wallet this breaking the transaction chain
- Launched on Indiegogo crowd funding website November 2013.
- Tweet from one prominent backer "Its just money laundering software"


Dark Wallet
chrome-extension://ffdpokjjdocmipkkabfankangimmmobi/html/index.html#/wallet
Dark Wallet
Wallet
Send
Contacts
Lobby
MyName
Pockets on my wallet
All
default
change
Name your pocket.
New Pocket
My multisig funds
Unsystem
Multisig 3
New Multisig fund
Watch-only pockets
My smartphone
My cold wallet
Add watch-only pocket
default 0 BTC
History
Addresses
Actions
Stealth Address
Master Address
Name
Address
unused
1NusgSy7uaowhGUM79bQFxkqYiUun31YM8
unused
18oxn1wjF7Q1VeFoQ2p3T8DyBJg65rDRjN
unused
15JZoCeBhWnf9t1BAoTTYMUtkHjbYwg3Z
unused
12ph7E7ubMcpmrfta4PHSzXNd2oggKiJBh
unused
16WMoY6thNa9iShBThrprkQimP7cHH3kQN
New address
Receiving transaction (+0.36 BTC)
55%
Sending transaction (-0.36 BTC)
55%
You have a spend approval request on the "Unsystem" multisig fund
2 out of 5 signatures still needed
You have been invited to the "dark wallet" multisig fund
Click for more info
Go to history...
Create new wallet...

Retention & Realisation

- Decisions – potential large source of funds for an LEA (eg ARIS)
- Do you retain it as a CC or realise it back into a fiat currency?
- Basis for decision – what is your purpose? Make money for the state? Deprive criminal of the assets?
- Irish example – Ethereum ICO
- Legal challenges. How do you realise it legally? Suspects agreement.
- How do you it technically? ie: Use of exchanges.(1)
- Realisation – costs
- Auction of Cryptoassets – Sell actually wallet whole
- Screening of bidders – access to legitimate funds
- Effect on the market – large sums being introduced can affect the value
- Moral Implications – anonymous assets – should they be re-introduced into the market. Take the hit?

Retention & Realisation

- Concerns
- Storage – how do you hold it securely long term? (2)
- Kidnap Policy
- Paper Wallets – Private & Public Key printed together – Offline Storage – generator – bitcoinpaperwallet.com
- Physical storage of hardware devices – Trezor, Keepkey, Ledger, etc
- Insurance – most LEAs will not be insured to cover in office storage
- 3rd party storage companies – difficulty in vetting – underwritten storage
- Staff safety – access to recovery phrases (3)
- Volatility - Overall CC market capitalisation lost 3/4s of value since January 2018 peak from $800B to $200B
- Change of Laws to authorise detention, realisation, etc

Retention & Realisation

- Seized devices – potential ICOs yet to commence trading
- Case Example CAB V Mannion (2018) IEHC 729 (17 December 2018)
- 7th November 2014 – Value US $350
- 27th July 2016 (sold) – Value US $25,416 – Decision
- 22nd March 2017 (hearing) – Value US $83,881
- 13th January 2018 (peak) – Value US $2,789,374
- 16th April 2018 (submissions) – Value US $1,030,482
- 17th December 2018 (judgement) – Value US $192,212
- After Seizure of the device the Cryptoasset "Forks". Have you seized the fork asset also? What is the legal position?

Priceless Vs Price Less

Forks & Airdrops

Forks

- We explained earlier that many cryptoassets operate on the basis of the community's 'consensus' for whether a transaction is valid
- When a significant minority of the community want to do something different, they may create a 'hard fork' in the blockchain. A fork may also occur when the person who created a 'smart contract' needs to change the rules in the smart contract.
- Before the fork occurs there is a single blockchain and both cryptoassets use the same blockchain up to the point of the fork. At the point of the fork, a second blockchain (and therefore a new cryptoasset) is created.
- The blockchain for the original cryptoassets and the new cryptoassets have a shared history up to the fork. If you held tokens of the cryptoasset on the original blockchain, after the fork you will still hold equal numbers of tokens on both blockchains.

Airdrops

- An airdrop is the distribution of tokens or other cryptoassets to individuals or businesses. For example, tokens may also be provided as part of a marketing or advertising campaign where certain people may be selected to receive tokens.
- These may be provided on the basis that they advertise the token or by way of a referral programme. Other airdrops may involve tokens being provided automatically due to other tokens being held by the individual: sometimes all that is required to become eligible is to register to take part in the airdrop.

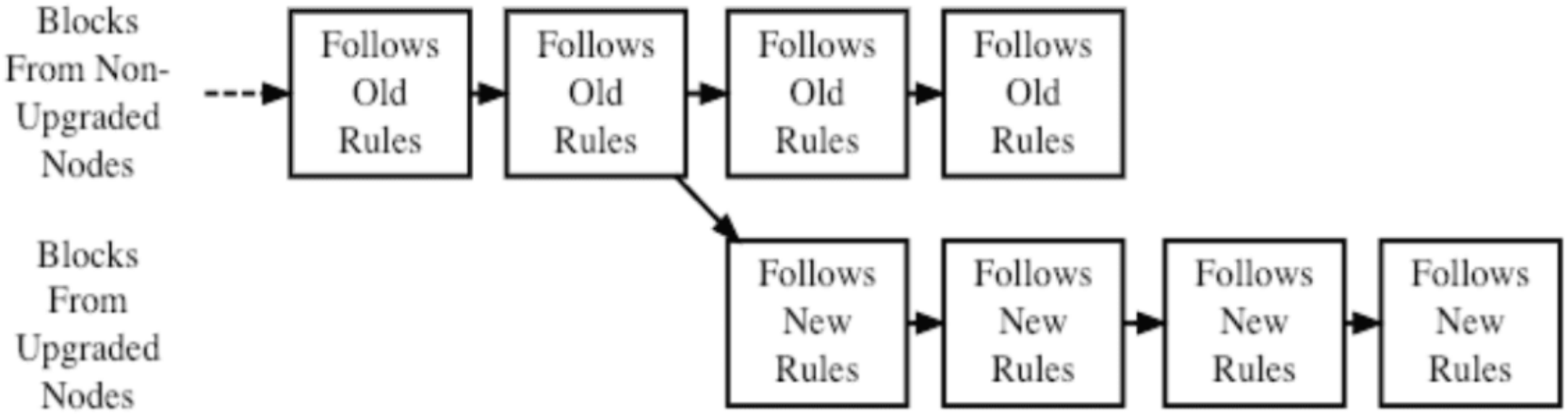
Glossary Terms

- Bitcoin Dust – refers to smaller amounts of bitcoin in a wallet or address where the monetary value is so small it is even lower than the transaction fee required to spend it. It makes the transaction impossible to process
- Hard Fork - a radical change to the protocol that makes previously invalid blocks/transactions valid (or vice-versa). All nodes or users upgrade to the latest version of the protocol software. It is a permanent divergence from the previous version of the blockchain, and nodes running previous versions will no longer be accepted by the newest version. This essentially creates a fork in the blockchain: one path follows the new, upgraded blockchain, and the other path continues along the old path.

Glossary Terms

- Why does a Hardfork happen?
- 1 - To correct important security risks found in older versions of the software, 2 - add new functionality, 3 - to reverse transactions (as in the case with the hard fork to reverse the hack on the DAO (decentralized autonomous organization) in the Ethereum blockchain).
- Following the hack on the DAO, the Ethereum community almost unanimously voted in favor of a hard fork in order to roll back transactions that siphoned off tens of millions of dollars worth of digital currency by an anonymous hacker. The hard fork also allowed DAO token holders to get their ether funds returned to them.
- Did not unwind the network's transaction history. It relocated the funds tied to The DAO to a newly created smart contract sole purpose of letting the original owners withdraw them.

OFFICIAL



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

Glossary Terms

- Soft Fork - a change to the software protocol where only previously valid blocks/transactions are made invalid. Old nodes will recognize the new blocks as valid – therefore it is backward-compatible.
- Only requires a majority of the miners upgrading to enforce the new rules. Compared to the hard fork which requires all nodes to upgrade and agree on the new version.
- Soft forks have been used on the Bitcoin and Ethereum blockchains, and others, to implement new and upgraded functionalities that are backwards compatible

OFFICIAL

Glossary Terms

- Virtual Asset Service Provider (VASP) – FATF describes them as "any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:
- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets; transfer of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Glossary Terms

- Wash Trade – form of known market manipulation also used in crypto-assets exchanges where an individual sells and buys the same instruments to create an artificial activity in the market place.
- Individual will place a sell order. Then he would place a buy order to buy from himself. Or vice versa. Why?
- To create false impression that the item is more in demand than it actually is, or
- To generate commission fees for brokers so that they receive funds for something which they cannot openly be paid
- It is illegal in many countries

Glossary Terms

- Custodian Wallet Providers -is **defined** as "an entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies."
- Virtual Currencies - a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency, and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically.

Greg Kelly

HMRC FRAUD INVESTIGATION SERVICE

MONEY LAUNDERING CRYPTO ASSET SME

ECONOMIC CRIME OPERATIONS

Threats posed to Criminal Investigations by use of Cryptoassets

FATF Recommendations & Regulations

- "an unregulated payment instrument with manifold opportunities for exploitation for money laundering purposes"
- "they represent a powerful tool for criminals to covert, move and store illicit funds, out of the reach of LEAs"
- 19TH October 2018 FATF published revised recommendations for international standards on combatting Money Laundering & Terrorist Financing
- This amended FATFs New Technologies (Regulation 15) and added two new definitions

FATF Recommendations

- What are they? Comprehensive and consistent framework of measures which countries should implement to combat ML & TF.
- Why? In response to G20 request for clarification on crypto-assets in relation to ML & TF
- Regulation 15 – New technologies

Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to (a) the development of new products and new business practices, including new delivery mechanisms, and (b) the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks. To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.

FATF - New Definitions

- Virtual Asset

Virtual Asset A virtual asset is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.

- Virtual Asset Service Providers

Virtual Asset Service Providers Virtual asset service provider means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person: i. exchange between virtual assets and fiat currencies; ii. exchange between one or more forms of virtual assets; iii. Transfer of virtual assets; iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

- FATF FinTech and RegTech Initiative – platform available for governments and Private Sector to share initiatives and developments

Where are we vulnerable?

- Decentralised currencies – no central server, no central supervisory body = nobody monitors transactions (no SARS) between peers for compliance
- Legal Framework – no supervision for CC exchanges, ATMs and wallet providers.
- Anonymity – CCs allow high speed movements of funds without disclosing true identity of owners. Cross jurisdiction risk high as internet based.
- Awareness – Most LEAs are in the dark as to the actual level of usage of CCs within their own sphere of intelligence
- Education – Staff awareness and training for understanding of CCs

Continuing & Evolving Threats

- Stablecoins
- Initial Coin Offerings
- Bitcoin ATMs
- Bitcoin Traders
- E-wallets
- Gift Cards
- Pre-Paid Crypto Cards
- Use of Crypto Assets to evade sanctions
- Off Chain Transactions
- SIM Swapping

Stable Coins

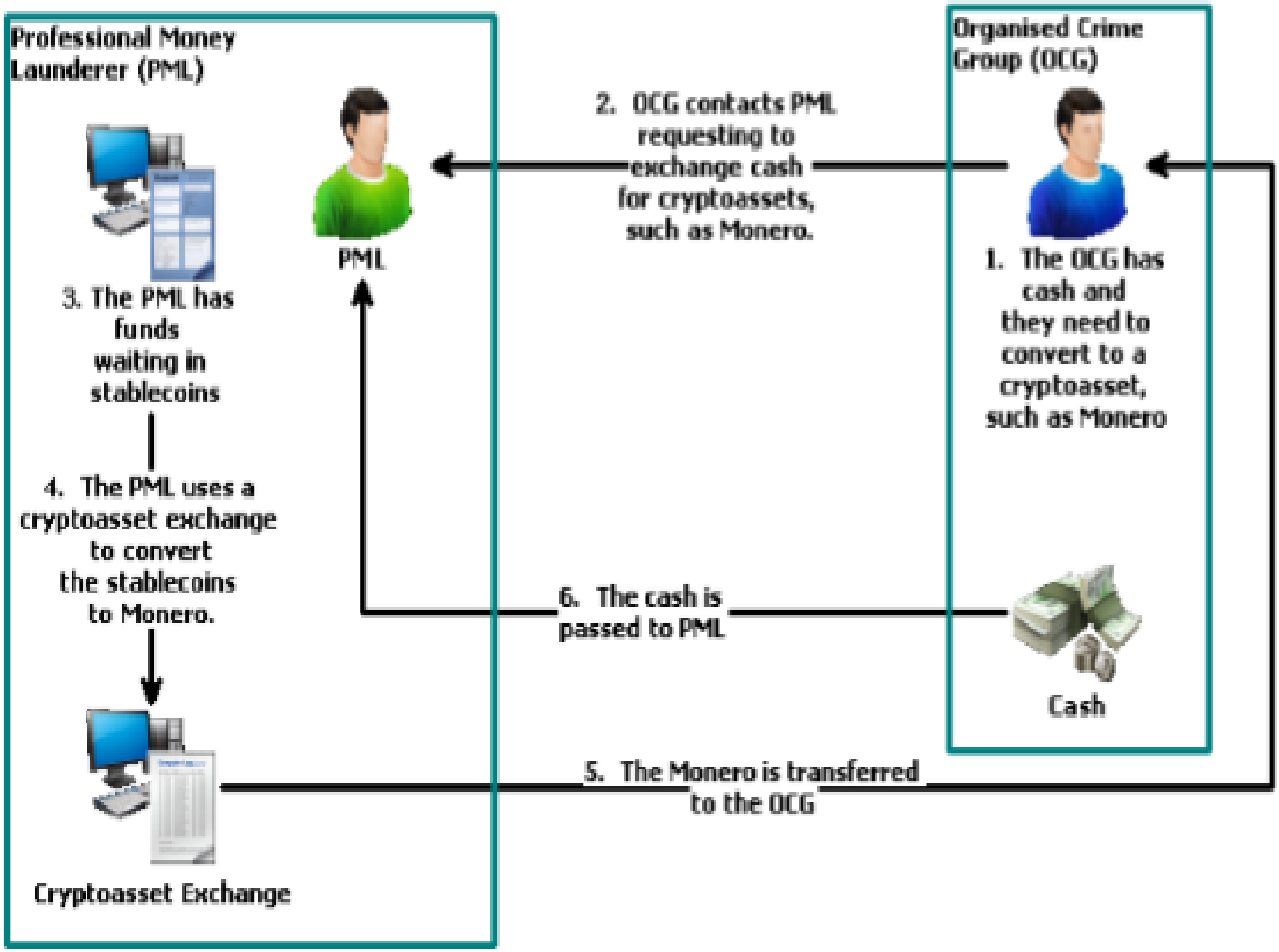
- Pseudo anonymous cryptoasset specifically designed to minimise price volatility (1)
- Minimise price volatility through having value pegged to a backing asset – FIAT currency or to an exchange commodity such as gold.
- The ratio will be fixed ie: 1 for 1
- Currently 57 Stablecoins in use or development
- Can be traded on an exchange or used to transfer value

Name	Symbol	Market Capitalisation	Circulating Supply	24hr Trade Volume	Peg/Ratio	Collateral
Tether (USDT)		£1.3bn	1.7bn	£1.7bn	US Dollar/1:1	US Dollar
DAI (DAI)		£53m	67m	£3m	US Dollar/1:1	Ethereum (ETH)
BitCNY (BITCNY)		£15m	142m	£12m	Chinese Yuan/1:1	Bitshares (BTS)
STASIS EURS (EURS)		£10m	12m	£287k	Euro/1:1	Euro
Digix Gold Token (DGX)		£2m	63k	£62k	1 gram of Gold/1:1	Gold

- Value and use of Stablecoins is at risk if – (a) the value of the backing asset changes, or (b) there is a loss of trust in the issuer (4)
- Other Stablecoins use other cryptoassets as collateral or algorithims to control value depending on market conditions
- Stablecoins are pseudo anonymous – transactions on blockchain can be viewed and traced but owner of each address is not revealed
- Not currently aware of any privacy focused Stablecoins ie like Monero

Legitimate use of Stablecoins

- Most popular use is to exit trading positions from cryptoassets that have a volatile value (5)
- Carried out via a cryptoasset exchange
- Useful if trader uses a cryptoasset exchange that does not have a FIAT currency to safeguard funds from changes in value or if the trader does not want to convert funds held in cryptoassets into FIAT.
- Can be used as a currency (6)
- Example of potential use by a PML


Professional Money Launderer (PML)
PML
3. The PML has funds waiting in stablecoins
4. The PML uses a cryptoasset exchange to convert the stablecoins to Monero.
Cryptoasset Exchange
2. OCG contacts PML requesting to exchange cash for cryptoassets, such as Monero.
Organised Crime Group (OCG)
1. The OCG has cash and they need to convert to a cryptoasset, such as Monero
6. The cash is passed to PML
Cash
5. The Monero is transferred to the OCG

Benefits to the Professional Money Launderer

- Funds are protected against changes in value
- Funds kept outside of traditional banking system
- Unknown variables – how are they held – hardware device, custodian wallet on an exchange

Initial Coin Offerings

- FCA report (12/09/2017) – a digital way of raising funds from the public using a Cryptocurrency/Virtual Currency. (token sale or coin sale)
- High risk speculative investments
- Issue a “coin” or “token” that is related to a specific firm or project
- Digital token can represent – a share in a firm (equity token), a prepayment voucher for future services (utility token) or possibly have no discernible value
- Generally they are at early stage of development
- Similar in nature to Initial Public Offerings (IPOs)

RISKS

- Unregulated in most countries
- Lack of protection for the investor
- Volatility of price
- Fraud potential – Ponzi scheme – estimated 80%
- Lack of comprehensive documentation
- Experimental business models

Name	Symbol	Added	Market Cap	Price	Circulating Supply	Volume (24h)	% 24h
CENTERCOIN	CENT	1 day ago	$?	$0.047062	? *	$29,205	?
SnapCoin	SNPC	1 day ago	$?	$0.069220	? *	$52,900	?
ICOBay	IBT	1 day ago	$?	$0.000432	? *	$40	?
ROIyal Coin	ROCO	1 day ago	$?	$0.277241	?	$43,755	?
BitMax Token	BTMX	1 day ago	$?	$0.016401	? *	$?	2.90%
StrongHands Masternode	SHMN	1 day ago	$?	$0.564861	?	$1,650	?
DogeCash	DOGEC	2 days ago	$?	$0.080105	?	$6,718	1.80%
Almeela	KZE	2 days ago	$?	$0.183906	? *	$59,413,327	-5.05%
Ultiledger	ULT	2 days ago	$?	$0.006658	? *	$18,918	-2.24%
ROMToken	ROM	5 days ago	$?	$0.000107	? *	$?	1.94%
Winco	WCO	5 days ago	$?	$0.003615	? *	$40,447	-4.69%
ProxyNode	PRX	5 days ago	$?	$0.140508	?	$26,774	36.60%
Atomic Wallet Coin	AWC	5 days ago	$?	$0.044077	? *	$504	-27.12%
Impleum	IMPL	5 days ago	$?	$0.041921	?	$7,807	24.11%
AgaveCoin	AGVC	5 days ago	$?	$0.009526	? *	$35,695	-3.57%
Footballcoin	XFC	6 days ago	$?	$0.005181	? *	$8,412	-0.35%
HedgeTrade	HEDG	6 days ago	$?	$0.138367	? *	$218,651	-1.32%
Stronghold Token	SHX	6 days ago	$?	$0.003636	? *	$11,402	0.47%
USDCoin	USC	6 days ago	$?	$1.02	? *	$14,557,798	0.45%
QUINADS	QUIN	6 days ago	$?	$0.000006	? *	$10,835	-7.95%
Fountain	FTN	7 days ago	$?	$0.033601	? *	$152,918	-1.18%
Lambda	LAMB	7 days ago	$?	$0.013827	? *	$1,284,391	20.92%

WARNING SIGNS/QUESTIONS

- The 10 biggest ICO scams are worth $700 MILLION
- Loop X – exit scam was worth $4.5M
- People behind the issue – do they have experience in the industry, CV?
- Promotional material – has no real content – purely buzz words and catchphrases
- The ICO has no cap or maximum limit
- Why do they need to issue an ICO to fund raise?
- Is there a need for a token?
- Does the business model make sense?
- Look at the technology being used – is it suited to purpose? How will the token work? Economic understanding?
- In which jurisdiction are they looking to incorporate? One with a high regulatory barrier for AML & banking licences – Switzerland, Singapore, Malta, Korea?

Cryptocurrency ATMs

- Used to buy and sell a range of Cryptocurrencies – Bitcoin, Bitcoin Cash, Ethereum, Litecoin and Dash
- Ease of use.
- ID limit £500
- £20,000 daily transaction limit per customer
- www.coinatmradar.com
- Unregulated in most countries
- Sale and purchase of machines open to abuse also
- Attractive to money mule groups – move away from money remittance transfer services – Western union, etc.
- Spanish Guardia Civil case – drug trafficking funds paid in for Crypto at ATMs, split funds and multiple deposits – estimated 200,000 Euros p/m – Euro 3 million in total

ATM Operators

- Responsibilities of ATM Controller
- Workings of the ATM – accessible information
- KYC Requirements
- Verification Levels
- AMLD5 – ramifications obligation to report suspicious activity – ML and TF

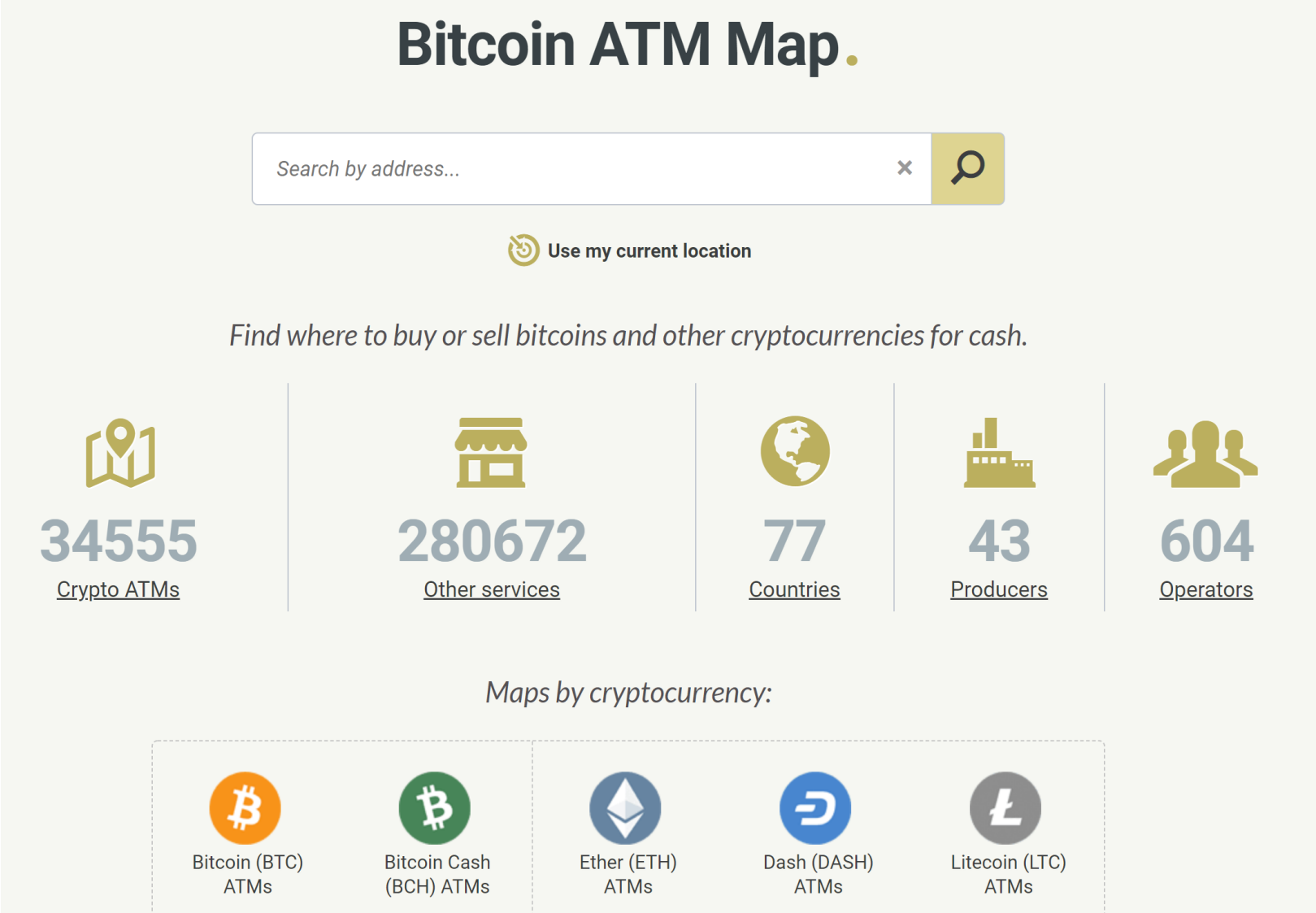
2018 View


Bitcoin ATM Map.
Use our map to find bitcoin or other cryptocurrency ATM locations as well as various alternative crypto-cash exchange services.
4182
Crypto ATMs
141842
Other services
75
Countries
42
Producers
525
Operators
Submit new ATM
Submit business to host ATM
Search by cryptocurrency:
Bitcoin (BTC) ATMs
Bitcoin Cash (BCH) ATMs
Ether (ETH) ATMs
Dash (DASH) ATMs
Litecoin (LTC) ATMs

2021 View


Bitcoin ATM Map.
Search by address...
Use my current location
Find where to buy or sell bitcoins and other cryptocurrencies for cash.
25935
Crypto ATMs
279325
Other services
74
Countries
44
Producers
625
Operators
Maps by cryptocurrency:
Bitcoin (BTC) ATMs
Bitcoin Cash (BCH) ATMs
Ether (ETH) ATMs
Dash (DASH) ATMs
Litecoin (LTC) ATMs

2022 View


Bitcoin ATM Map.
Search by address...
Use my current location
Find where to buy or sell bitcoins and other cryptocurrencies for cash.
34555
Crypto ATMs
280672
Other services
77
Countries
43
Producers
604
Operators
Maps by cryptocurrency:
Bitcoin (BTC) ATMs
Bitcoin Cash (BCH) ATMs
Ether (ETH) ATMs
Dash (DASH) ATMs
Litecoin (LTC) ATMs

2018 World Map

2021 World Map

General map:

Submit a new ATM Location

Become an ATM Host

2022 World Map

General map:

Submit a new ATM Location

Become an ATM Host

Countries with most ATMs 2022

- 30, 469 ---------- United States
- 2,205 ---------- Canada
- 205 ---------- El Salvador
- 198 ---------- Spain
- 142 ---------- Switzerland

- Countries on this course
- Saudi Arabia ---------- 1
- United Arab Emirates --------- 1
- Lebanon ---------- 5

2018 World Countries

Bitcoin ATMs by Country.

Bitcoin ATMs are installed in many countries in the world. The current distribution of installations accross the countries can be found on The Chart of Bitcoin ATM number by Country or Bitcoin ATM installations by Continent.

- United States • (2515 locations)
- Canada • (706 locations)
- Austria • (265 locations)
- United Kingdom • (214 locations)
- Spain • (82 locations)
- Czech Republic • (65 locations)
- Australia • (54 locations)
- Ukraine • (10 locations)
- Malaysia • (10 locations)
- Singapore • (9 locations)
- Taiwan • (8 locations)
- Israel • (8 locations)
- Argentina • (8 locations)
- VietNam • (7 locations)
- Thailand • (2 locations)
- Germany • (2 locations)
- Saudi Arabia • (2 locations)
- Turkey • (1 location)
- Uganda • (1 location)
- South Korea • (1 location)
- Albania • (1 location)
- Russian Federation • (51 locations)
- Switzerland • (46 locations)
- Italy • (38 locations)
- Slovakia • (37 locations)
- Hong Kong • (32 locations)
- Romania • (28 locations)
- Poland • (28 locations)
- Colombia • (27 locations)
- Netherlands • (23 locations)
- Finland • (22 locations)
- Croatia • (6 locations)
- South Africa • (5 locations)
- Serbia • (5 locations)
- Liechtenstein • (3 locations)
- Malta • (3 locations)
- Portugal • (3 locations)
- Kosovo • (3 locations)
- Kazakhstan • (3 locations)
- Bulgaria • (3 locations)
- Chile • (3 locations)
- San Marino • (1 location)
- Guatemala • (1 location)
- Armenia • (1 location)
- Aruba • (1 location)
- Bahamas • (1 location)
- Barbados • (1 location)
- Bosnia and Herzegovina • (1 location)
- Djibouti • (1 location)
- France • (1 location)
- Iceland • (1 location)

- Greece • (20 locations)
- Slovenia • (14 locations)
- Hungary • (12 locations)
- Belgium • (11 locations)
- Japan • (11 locations)
- Panama • (11 locations)
- Mexico • (11 locations)
- Georgia • (11 locations)
- Dominican Republic • (10 locations)
- Ecuador • (3 locations)
- Guam • (2 locations)
- Norway • (2 locations)
- Brazil • (2 locations)
- Costa Rica • (2 locations)
- Denmark • (2 locations)
- New Zealand • (2 locations)
- Ireland • (2 locations)
- Estonia • (2 locations)
- Saint Kitts and Nevis • (1 location)
- Indonesia • (1 location)
- Anguilla • (1 location)
- Kenya • (1 location)
- Latvia • (1 location)
- Mongolia • (1 location)
- Peru • (1 location)
- Philippines • (1 location)
- Zimbabwe • (1 location)

2021 World Countries

Bitcoin ATMs by Country.

Bitcoin ATMs are installed in many countries in the world. The current distribution of installations accross the countries can be found on The Chart of Bitcoin ATM number by Continents and Countries.

- United States (2804 locations)
- Canada (685 locations)
- Austria (276 locations)
- United Kingdom (225 locations)
- Spain (85 locations)
- Czech Republic (67 locations)
- Russian Federation (60 locations)
- Switzerland (52 locations)
- Italy (43 locations)
- Slovakia (42 locations)
- Taiwan (9 locations)
- Argentina (9 locations)
- Singapore (9 locations)
- Israel (8 locations)
- Germany (8 locations)
- VietNam (7 locations)
- South Africa (6 locations)
- Serbia (6 locations)
- Croatia (6 locations)
- Japan (5 locations)
- Saudi Arabia (2 locations)
- Brazil (2 locations)
- Costa Rica (2 locations)
- San Marino (1 location)
- South Korea (1 location)
- Uganda (1 location)
- Albania (1 location)
- Saint Kitts and Nevis (1 location)
- Djibouti (1 location)
- Anguilla (1 location)
- Poland (36 locations)
- Hong Kong (36 locations)
- Colombia (33 locations)
- Romania (30 locations)
- Netherlands (25 locations)
- Greece (23 locations)
- Australia (21 locations)
- Finland (20 locations)
- Slovenia (15 locations)
- Hungary (14 locations)
- Ireland (4 locations)
- Liechtenstein (4 locations)
- Portugal (4 locations)
- Estonia (4 locations)
- Bulgaria (4 locations)
- Malta (4 locations)
- Ecuador (3 locations)
- Thailand (3 locations)
- Kosovo (3 locations)
- Kazakhstan (3 locations)
- Armenia (1 location)
- Aruba (1 location)
- Bahamas (1 location)
- Barbados (1 location)
- Bosnia and Herzegovina (1 location)
- Botswana (1 location)
- France (1 location)
- Philippines (1 location)
- Guatemala (1 location)
- Iceland (1 location)

Mexico • (12 locations)

Panama • (12 locations)

Belgium • (12 locations)

Dominican Republic • (11 locations)

Malaysia • (10 locations)

Ukraine • (10 locations)

Georgia • (10 locations)

Chile • (3 locations)

Guam • (2 locations)

Turkey • (2 locations)

New Zealand • (2 locations)

Norway • (2 locations)

Denmark • (2 locations)

Peru • (2 locations)

Indonesia • (1 location)

Andorra • (1 location)

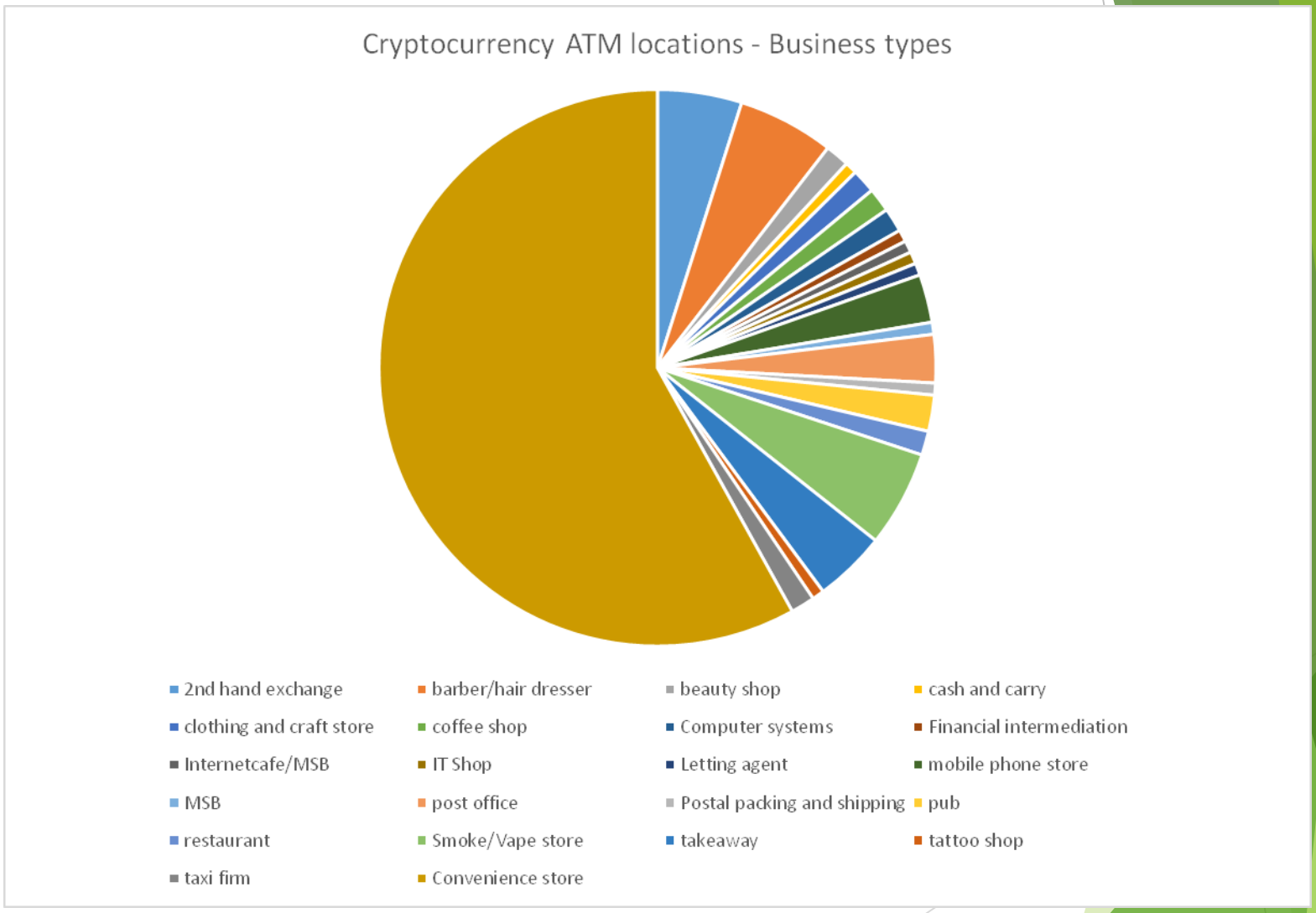
Kenya • (1 location)

Latvia • (1 location)

Mongolia • (1 location)

Zimbabwe • (1 location)

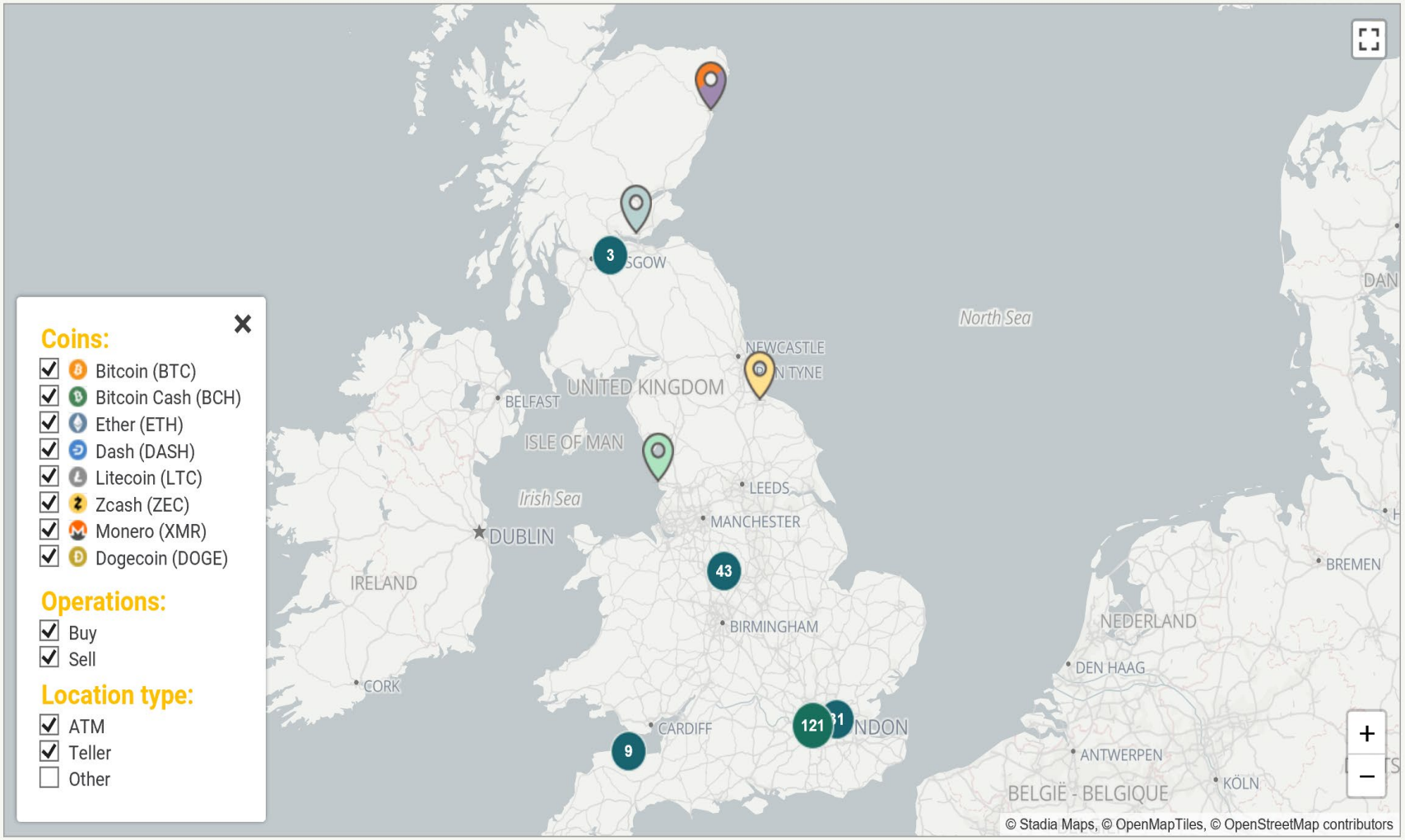
Cryptocurrency ATMs UK



OFFICIAL

Bitcoin ATMs in United Kingdom.

Total number of Bitcoin ATMs / Tellers in United Kingdom: 214



List of major cities in United Kingdom with bitcoin ATM installations: .

Aberdeen 1

Birmingham, UK 18

Bradford 1

Brighton UK 4

Bristol 3

Cardiff 5

Chelmsford 2

Chudleigh 1

Coventry 1

Dartford 1

Derby 1

Eastbourne 1

Edinburgh 2

Exeter 1

Glasgow 3

Harrow 2

Kingsbridge 1

Kingston upon Hull 1

Leeds 1

Leicester 2

London, UK 135

Manchester (UK) 18

Newport 1

Penzance 3

Peterborough 1

Portsmouth 2

St Albans 1

Swansea 1

Bitcoin ATMs in United Kingdom.

Total number of Bitcoin ATMs / Tellers in United Kingdom: 225

List of major cities in United Kingdom with bitcoin ATM installations:.

Aberdeen 1

Birmingham, UK 19

Bradford 1

Brighton UK 4

Bristol 3

Cardiff 5

Chelmsford 3

Chudleigh 1

Coventry 1

Derby 1

Eastbourne 1

Edinburgh 2

Exeter 1

Glasgow 2

Harrow 2

Kent 1

Kingsbridge 1

Kingston upon Hull 1

Leeds 1

Leicester 2

London, UK 142

Manchester (UK) 21

Newcastle upon Tyne 1

Newport 1

Penzance 3

Peterborough 1

Portsmouth 2

St Albans 1

Bitcoin ATMs in United Kingdom.

Total number of Bitcoin ATMs / Tellers in United Kingdom: 164

List of major cities in United Kingdom with bitcoin ATM installations:

Aberdeen 1

Basildon 1

Belfast 2

Birmingham, UK 22

Brighton UK 2

Bristol 1

Cambridge 1

Cardiff 6

Chelmsford 3

Derby 1

Dundee 1

Edinburgh 3

Glasgow 2

Harrow 2

Kingsbridge 1

Kingston upon Hull 2

Leeds 2

Leicester 2

London, UK 90

Manchester (UK) 13

Newcastle upon Tyne 1

Oxford 1

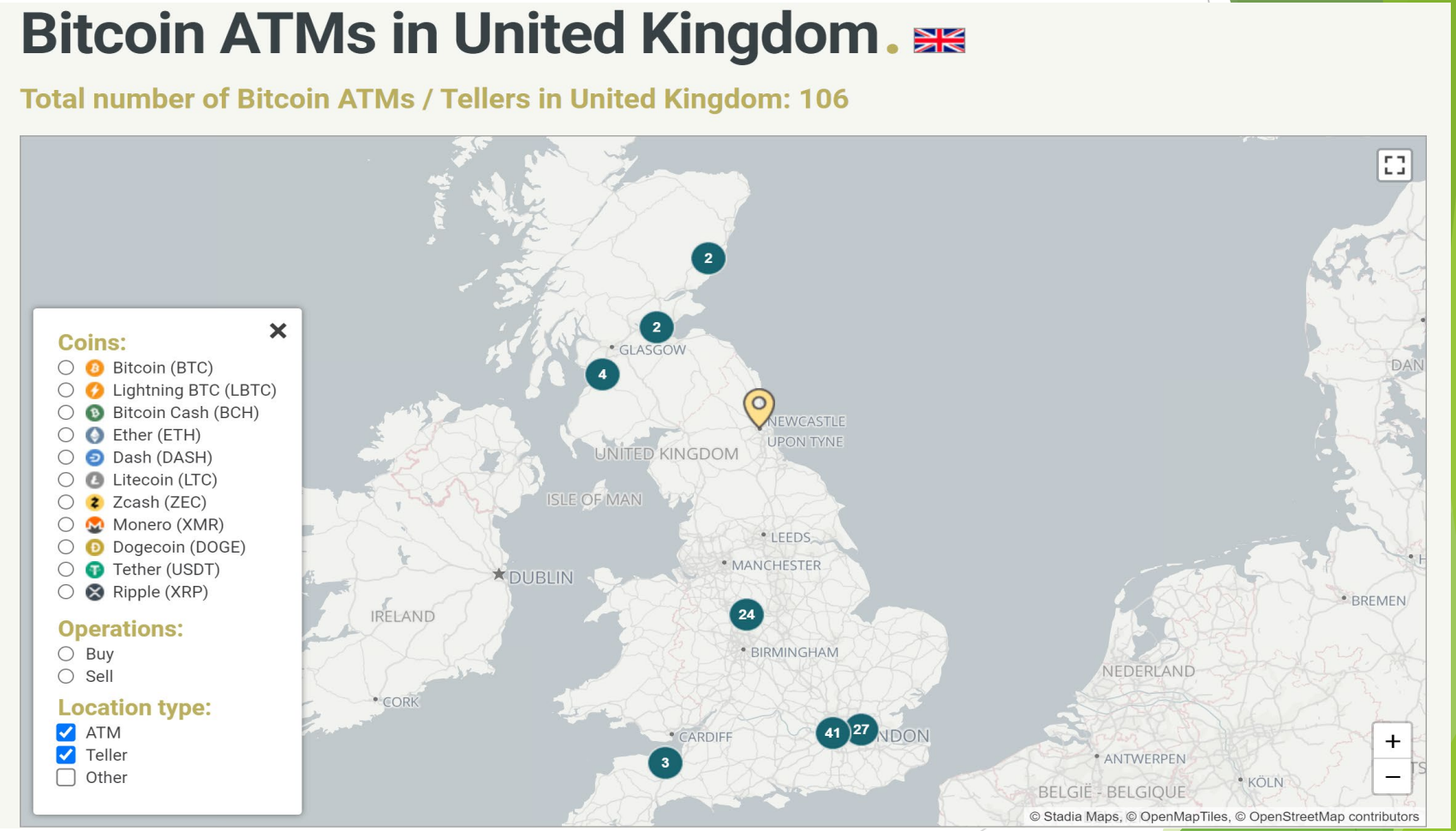
Plymouth 1

Preston 1

Southampton 1

Southend-on-Sea 1

2022 UK ATMs


Bitcoin ATMs in United Kingdom.
Total number of Bitcoin ATMs / Tellers in United Kingdom: 106
Coins:
Bitcoin (BTC)
Lightning BTC (LBTC)
Bitcoin Cash (BCH)
Ether (ETH)
Dash (DASH)
Litecoin (LTC)
Zcash (ZEC)
Monero (XMR)
Dogecoin (DOGE)
Tether (USDT)
Ripple (XRP)
Operations:
Buy
Sell
Location type:
ATM
Teller
Other
2
2
4
GLASGOW
NEWCASTLE UPON TYNE
UNITED KINGDOM
ISLE OF MAN
LEEDS
MANCHESTER
DUBLIN
IRELAND
24
BIRMINGHAM
CORK
CARDIFF
41
27
3
NEDERLAND
BREMEN
ANTWERPEN
KÖLN
BELGIË - BELGIQUE
© Stadia Maps, © OpenMapTiles, © OpenStreetMap contributors

List of major cities in United Kingdom with bitcoin ATM installations:.

Aberdeen 1	Chelmsford 2	Manchester (UK) 9
Basildon 1	Dundee 1	Newcastle upon Tyne 1
Belfast 1	Edinburgh 3	Oxford 3
Birmingham, UK 13	Glasgow 2	Plymouth 2
Brighton UK 1	Kingsbridge 1	Reading 1
Bristol 1	Leeds 1	Southampton 1
Cardiff 2	London, UK 58	Southend-on-Sea 1

E-wallets

- Also known as Electronic Money Institutions (EMIs) – Paypal, Skrill
- Often they offer prepaid cards also
- Opening – internet access, email address, credit or debit card
- Accessed – Laptop, mobile phone, tablet, PC
- Free to open. Easy to open – less than 1 hour
- Sender E-wallet to Recipient E-wallet (amount debits Senders bank/card)
- Recipient – credit to bank, load onto prepaid card, spend on
- Unless LEA knows of existence of E-wallet money can be dispersed
- Useful tool for businesses to suppress card sales on-line
- Businesses (in the UK) do not have to set up Merchant Enquirer accounts to accept payments from E-wallets
- Reliance on providers of E-wallets to report suspicious activities ie large credit payments

Privacy Crypto Wallets

- They provide an opportunity to maximise your privacy when using Crypto
- Multiple brands available on various platforms all offering similar levels of encryption
- Samourai Mobile Wallet - advertised as “a bitcoin wallet for the streets”
- Wasabi Desktop Wallet - an open source non-custodial Btc privacy wallet
- Bitlox Hardware Wallet - supports only Btc but developing devices for Ethereum and other cryptos
- Rahakott Web Wallet – anonymous web multi-currency wallet. Supports Btc, Bitcoin Cash, Ethereum, Litecoin, Monero, Zcash and Dash

WASABI WALLET

Samourai


Rahakott
Log in
Create wallet
EN
Anonymous multicurrency cryptowallet
+ mixer
Reliable wallet that will not tip off about you. Create just in 15 seconds, without an email or phone number.
Create wallet *
* It is absolutely free

Pre-paid Cryptocurrency Cards

- Cryptocurrency linked to a wallet is converted into FIAT and loaded onto a pre-paid card
- January 2018 VISA Europe withdrew services to WaveCrest
- Minimal effect to OCGs as other ways to cash out
- US based CC card providers unaffected
- Study of usage – 50% USA, 35% Europe and 15% Asia
- May 2018 Wirex launched Cryptocurrency Debit Card in Europe
- Alternative Payment Platform – CONTIS
- Regulation should be covered by 5th AMLD (to be introduced in Europe)
- Example 1 – Spanish Police – drug sales. BTC loaded onto PP cards
- Example 2 – Finnish Police – DarkWeb market place trader used CC PP cards to launder E280,000 (E100,000 from ATMs)
- Example 3 – Norwegian Customs – suggest CCPP cards used to launder funds. 74% of cards used for less than 2 months
- The larger the withdrawal the less the life span of usage

- Crypto Debit card company who offers a prepaid card
- Offer – Bitcoin, Ether, Dash and NEM
- Services offered in multiple languages – English, Russian, Chinese, portugese, French, Arabic, Japanese and Lithuanian
- Payment Methods – Bank Transfer, Visa, Mastercard, Giropay, Skrill, SEPA Credit Transfer, Sofort by Klarna

Ca

Crypto Asset Gift

- Launched 2017 Gift cards can be redeemed instantly for cryptocurrency
- Value from 25, 50, 100, 200 and 500 Euros
- Only available currently – Bitcoin and Dash
- Available at 30,000 stores in Spain and Italy and currently expanding into Portugal and France 5,000 stores in each

Bitnovo cryptocurrencies Gift Cards

How Does it Work?

- Bitnovo is a Spanish company – sale of crypto assets and services
- Sixthcontinent is an Italian company – specialises in shopping/gift cards
- Access Sixthcontinent Website
- Choose a “Bitnovo” Gift Card
- Choose the amount you wish to purchase
- Complete payment process
- Redeem the card code in the Bitnovo App or on the website
- Insert PIN code and the number of your virtual wallet
- The Crypto Asset will arrive in your wallet in less than 30 minutes
- Looking to launch in Mexico, Brazil, Argentina and USA
- Bitnovo PIN Cashout App – allows use to sell crypto asset for cash
- User receives a PIN code within the app which is redeemable at 4,000 local stores for cash in Spain

Evasion of Sanctions

Four Iranian Banks Support Gold-Backed Cryptocurrency

Background

- Financial Tribune article dated 30th January 2019
- PayMon – developed by four banks in Iran
- Backed by Gold – Stablecoin. Government/State backed.
- Initial release of 1 BILLION tokens
- Iran in negotiations with Switzerland, South Africa, France, UK, Russia, Austria, Germany and Bosnia to conduct financial transactions in crypto
- In July 2018 it was reported that the country confirmed it would create it's own state-issued cryptocurrency to circumvent USA sanctions
- November 2018 – USA released new wave of sanctions – resulting effects – oil exports dropped, SWIFT disconnected from banks, OFAC added 700 officials to transaction watch-list
- Estimated to have cost Iran a $400B drop in GDP since these sanctions
- January 2019 Iranian lawmakers seek to introduce legislation to block the use of crypto for payments inside of the country

Iran Position

May 21, 2021
1:40 PM BST
Last Updated 8 months ago

Technology

Iran uses crypto mining to lessen impact of sanctions, study finds

LONDON, May 21 (Reuters) - Around 4.5% of all bitcoin mining takes place in Iran, allowing the country to earn hundreds of millions of dollars in cryptocurrencies that can be used to buy imports and lessen the impact of sanctions, a new study has found.

At its current level of mining, Iran's bitcoin production would amount to revenues close $1 billion a year, according to figures from blockchain analytics firm Elliptic.

Iran bans cryptocurrency mining for four months after blackouts

26 May 2021

An estimated 4.5% of all Bitcoin mining takes place in Iran

Iran has announced a four-month ban on the energy-consuming mining of cryptocurrencies such as Bitcoin after cities suffered unplanned blackouts.

President Hassan Rouhani told a cabinet meeting the main cause of the blackouts was a drought that had affected hydro-electric power generation.

But he said cryptocurrency mining, 85% of which is unlicensed, was draining more than 2GW from the grid each day.

An estimated 4.5% of all Bitcoin mining takes place in Iran.

According to analytics firm Elliptic, the activity allows the country to bypass sanctions and earn hundreds of millions of dollars in crypto-assets that can be used to purchase imports.

- **Bitcoin consumes 'more electricity than Argentina'**

Iran's banks were cut off from the global financial system and its oil exports plummeted, depriving it of a major source of hard currency and revenue, as a result of sanctions reinstated by the US in 2018 when then President Donald Trump abandoned a landmark nuclear deal.

June 22, 2021
2:21 PM BST
Last Updated 7 months ago

Technology

Iran seizes 7,000 cryptocurrency computer miners, largest haul to date

2 minute read

Reuters

DUBAI, June 22 (Reuters) - Iranian police have seized 7,000 computer miners at an illegal cryptocurrency farm, their largest haul to date of the energy-guzzling machines that have exacerbated power outages in Iran, state media reported on Tuesday.

In late May, Iran banned the mining of cryptocurrencies such as Bitcoin for nearly four months as part of efforts to reduce the incidence of power blackouts blamed by officials on surging electricity demand during the searingly hot and dry summer.

HELEN PARTZ

JAN 11, 2022

Iran to allow crypto payments for international trade: Report

Iran is reportedly looking to unlock opportunities for importers and exporters to use crypto in international deals.

The Central Bank of Iran, or CBI, and the Ministry of Trade have reached an agreement to link the CBI's payment platform to a trade system allowing businesses to settle payments using cryptocurrencies, the Mehr News Agency reported Monday.

Alireza Peyman-Pak, Iran's deputy minister of Industry, Mine and Trade and head of Iran's Trade Promotion Organization, or TPO, said that the new payment mechanism is expected to be finalized "within the next two weeks."

"We are finalizing a mechanism for operations of the system. This should provide new opportunities for importers and exporters to use cryptocurrencies in their international deals," Peyman-Pak reportedly said.

He added that the government should not be ignoring the economic and business opportunities of the crypto industry, referring to major private cryptocurrencies like Bitcoin (BTC):

The Iranian government is reportedly preparing a mechanism to enable the use of cryptocurrencies in international trade.

> **"All economic actors can use these cryptocurrencies. The trader takes the ruble, the rupee, the dollar, or the euro, which he can use to obtain cryptocurrencies like Bitcoin, which is a form of credit and can pass it on to the seller or importer. [...] Since the cryptocurrency market is done on credit, our economic actors can easily use it and use it widely."**

OFFICIAL

Venezuela

- December 2017 – Announcement made – supplement currency and help overcome US sanctions
- October 2018 – Venezuela launched - oil-backed cryptocurrency – Petro.
- Nicolas Maduro (President) claimed it raised $735M in it's first pre-sale day
- Government claims Petro is backed by oil, gas, gold and diamonds and is meant to overcome US and EU sanctions
- Petros will be "pre-mined" – produced and controlled by government
- Allocated 5 Billion Barrels of oil to back it – tied to the cost of a barrel of oil
- Offered for sale by FIAT "hard" currencies and other cryptos
- Each one sold at same cost
- Current price $62 a barrel – 100 million Petros = circa $6 Billion.
- US signed Executive Order barring US institutions from transactions using Petro.

Off Chain Transactions

- Transactions which occur on a cryptocurrency network which move value outside of the Blockchain.
- Increasing in popularity due to low/zero cost
- Normal transaction occurs - considered valid when the blockchain is modified to reflect the transaction on the public ledger.
- The transaction is validated and authenticated by participants, transaction details recorded on the block, result broadcast to the whole blockchain network – virtually irreversible.
- This kind of transaction can be reversed only after a majority of the network's hashing power comes to an agreement.
- Various types of “Off Chain” Transactions
- Simplest way - two parties exchange their private keys involving a fixed amount of crypto. The coins never leave the address/wallet, but the currency receives a new owner off-chain.
- Coupon-based payment mechanism. A purchases coupons in exchange for crypto, passes the code to B. B can then redeem them, in the same cryptocurrency or in different ones, depending on the coupon service provider.

Off Chain Transactions

- Third Party Guarantor – acts as guarantor and honours the transaction. (Similar to how payment processors like PayPal work)
- What are the benefits?
- Execute instantly - On-chain transactions can have a lengthy lag time depending upon the network load and number of transactions waiting in the queue to be confirmed
- No transaction fee (usually) - nothing occurs on the blockchain. No miners to validate the transaction. Attractive option especially if large amounts are involved.
- More Security & Anonymity - details not publicly broadcast. It is possible to identify a person by studying transaction patterns of on-chain transactions

SIM-SWAPPING

- Also known as SIM Hijacking
- ID theft where perpetrator creates a new SIM card for numbers and uses it for personal gain
- Original phone number user has no knowledge
- MO of Fraud
- Attacker calls telecom provider and convinces CS that he is actual owner by providing personal information 1
- Telecom company ports phone number to new SIM card which is sent to attacker (old SIM is cancelled)
- Attacker accesses crypto wallets and on-line banking and any synched accounts – reset passwords to compromise 2FA authentication
- Attackers stole over $100M USD from thousands of victims

2018 Position

Hackers Stole $1.7 Billion in Cryptocurrency Last Year

By Ionut Ilascu

January 29, 2019 11:06 AM

Cybercriminals going after digital coins had a good 2018, stealing a whopping $1.7 billion in cryptocurrency from exchange services, users, or investors. Different forms of scamming, extortion, hacking, and malware were the main methods used to get the money.

A report shared with BleepingComputer informs that cryptocurrency exchanges and infrastructure lost more than $950 million to hackers, with Korea and Japan being the home to most of the heists.

Exit scams lead the way

Exit scams are the top reason for cryptocurrency losses in 2018, says the report from CipherTrace, a company that offers anti-money laundering and blockchain forensics solutions.

One of the largest scams occurred in April, when Vietnamese cryptocurrency company Modern Tech launched an Initial Coin Offering (ICO) and raised $660 million from about 32,000 individuals. After a while, all operations stopped and the investors were left waiting for their returns.

Another notable scam involves a Vietnamese cryptocurrency mining endeavor called Sky Mining, whose founder and CEO disappeared with assets and mining rigs worth up to $35 million.

Hacking & SIM swapping for Cryptocurrency

Hacking and SIM awapping for cryptocurrency

According to the report, hacking their way to the money was another cause for users to lose digital coins The attacks targeted either the exchange services or focused directly on high-value users.

"In Japan, hackers pulled off the largest cryptocurrency heist in history, robbing users of a major cryptocurrency exchange of $530 million. This breach was followed in October by a $70 million theft from an exchange in Osaka," informs the report.

Some cybercriminals turned to the SIM swapping technique to steal a victim's phone number and thus get access to sensitive information used for two-factor authentication or two-step verification to access exchange accounts or wallets.

One way to achieve this is by bribing an insider at a mobile service provider to associate the victim's number to another SIM card, says lieutenant John Rose of the Silicon Valley REACT Task Force.

"If you're working at a mobile phone store and making $12 an hour and suddenly someone offers you $400 to do a single SIM swap, that can
seem like a pretty sweet deal," said the lieutenant.

By means of SIM swapping, a hacker last year was able to allegedly steal $23.8 million from a cryptocurrency investor.

Starting Point – Considerations for Every Country

- Legal Framework – each country needs to look at how they want to tackle the issues. Changes to law to support LEAs
- Regulation – 5th EU AMLD or own individual internal controls
- Strategy – Proactive or Reactive?
- Technology – constantly changing. Investment in latest computers, software, training packages. Blockchain advances.
- Awareness – basic level of training for all investigators. Small specialised teams to deal with more complex areas.

Impacts of Regulation in the UK?

- UK - Home Office Legislation changes on dealing with CCs? (1)
- The EU 5th Money Laundering Directives will bring regulation of Cryptocurrency Exchanges, Custodian Wallet Providers and Obliged Entities (2). Will it cover ATMs?
- Challenge 1 – number of SARs/STRs will increase – on-line gambling could create a tidal wave. (Scoping exercise of 6.5M SARs lodged only 10% investigated). Can LEAs cope with this?
- Challenge 2 – As regulation becomes stringent difficult for criminals to enter financial markets. Look outside of EU for jurisdictions with lax regs.
- Acceptance of the risk of ML using CCs by Governments growing as more cases arise.
- Also increased usage and acceptance of CCs without the need to cash in or exchange for real currency
- CCs – An Asset or a viable currency? (3)
- To improve as a transaction medium – maintain high security and speed up transactions.

Co-operation with Law Enforcement

- Some of the main operators will provide LEAs with information via the required legal gateway
- Bitnovo can track and lock gift cards if necessary to avoid abuse. Happy to provide LEAs with information through right channels
- Bitpay – claim to be global leader in Bitcoin payments and perform AML and KYC on customers. They do produce STRs on customers and monitor their usage of markets provided. Assistance provided to FBI and FIOD.
- Require – an Official signed LEA request sent to subpoenas@bitpay.com
- What can they provide – Transaction data – dates, times, amounts of USD or BTC, Merchant Contact Information – name, address and email, Limited Shopper Information (requires GDPR), Information provided by Merchant during on-boarding process – IP addresses from customer invoices

Trends 2021 -2022

- DarkNet Markets continue to thrive – close down one and it is replaced by another
- Encrypted Messaging – new apps giving higher level of encryption with all message being sent between OCGs
- Diversification by OCGS
- Crypto-Mining via hijacked computer power
- On-line Gambling sites being purchased or set up by OCGs – launder funds, stream of revenue
- Sanctions Evasion – Enforcement by OFAC and government agencies to increase in this area

Further Developments to watch

- DeFi – Decentralised Finance
- Represents a change in the cryptoasset ecosystem
- Operates off Smart Contract system on Ethereum
- Allows for a wide variety of products to be developed and offered which were previously only offered through CeFi (1)
- Early 2020 Ethereum based smart contracts held value worth $700 Million
- By December 2020 this had increased to £15 Billion
- Lending Platforms – connecting borrowers to lenders of crypto
- Collateral based – a user who wants to take out a loan needs to put up collateral (usually Ether)
- No identity require. No credit score.

Decentralised Exchanges - DEX

- Facilitate the buying, selling and swapping of cryptoassets between parties
- Accessed on-line
- They fall within the definition of a VASP for regulation purposes
- Orders are executed on-chain by Smart Contracts
- At no time do they take ownership of the cryptoassets
- The DEX arranges the contracts between the owners
- The users provide the liquidity which allows operation of system
- Concerns
- Location
- Autonomous Operation

Non-Fungible Tokens- NFTs

- Non-Fungible means that it is not interchangeable for another asset
- Ie: It is unique
- NFTs can be beneficially owned and are recorded in a similar manner to other cryptoassets
- It is a cryptographic record of ownership for a unique item which is encoded into a Distributed Ledger (Blockchain)
- They are intangible so not currently possessable, ie: not able to physically possess them under law
- Used in a variety of ways – collectibles (including artwork), gaming – EG: Cryptokitties, Intellectual property, Ownership of physical property, records and identity verification, financial documents

Non-Fungible Tokens- NFTs

- March 2021 – digital artist Beeple sold NFT of a piece of his digital art for $69.3M through Christies Auctions
- An original Banksy, Morons, was burnt in a livestream video after it had been tokenised. The NFT representing the video of the burning sold for $380,000.
- Jack Dorsey sold his first tweet as an NFT for $2.9M.
- Kings of Leon released an album as an NFT generating $2M in sales. For them they bypassed streaming and download markets and collected royalties directly
- NBA produced NBA Top Shot – limited edition virtual basketball cards. Trades exceeded $500M as of May21.
- June 2021 – Sir Tim Berners lee sold the source code for the internet via Sotheby's for $5.4M
- Cryptokitties – once created Dapper labs (creator) are the copyright owner and can decided how the image is used

Greg Kelly

HMRC Fraud Investigation Service

Money Laundering Cryptoasset SME

Economic Crime Operations