DIGITAL ASSETS

INVESTIGATIVE AND SEIZURE APPROACHES AND CONSIDERATIONS

JEFF T COOPER

DEPARTMENT OF THE TREASURY

DEFINITIONS

- *Digital financial assets* is a broad term that includes digital currencies as well as digital securities, digital commodities, and digital derivatives.

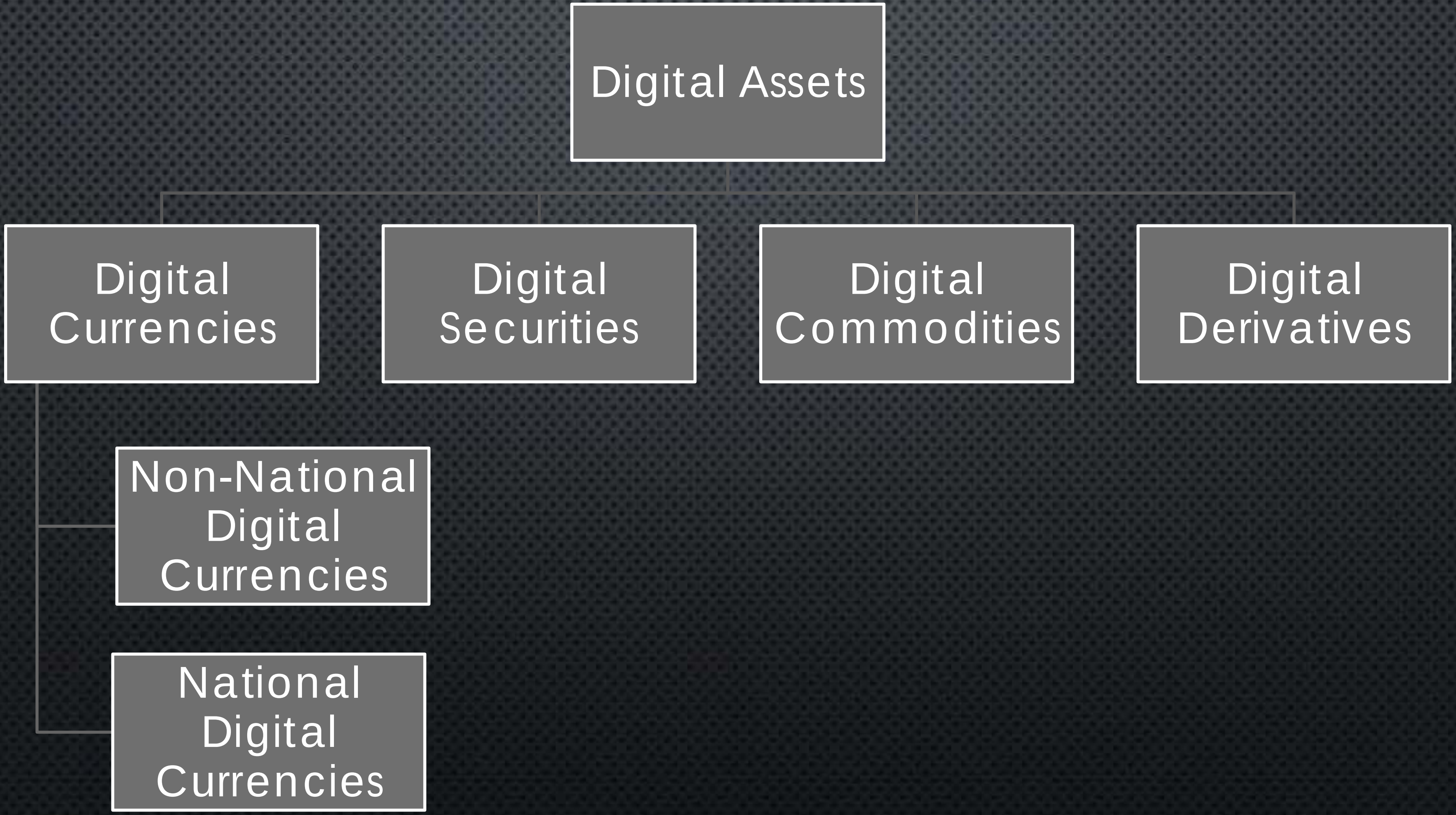
- *Digital currency* is
  - a digital representation of fiat currency that serves as legal tender and is issued by a jurisdiction,

  OR

  - certain virtual currency (NON-FIAT) that is neither issued nor guaranteed by any jurisdiction and is not legal tender in any jurisdiction. *[Note: most proposed stablecoins today exist here]*

- A so-called *'Stablecoin'* is
  - a digital asset designed to minimize the volatility of the price of the digital asset, relative to some other asset or basked of assets; this could be a peg to fiat money, exchange-traded commodities, or any other asset believed to be 'stable'. *[Ex: The Libra Association's proposed LBR]*

DIGITAL ECOSYSTEM



CRYPTO CHARACTERISTICS

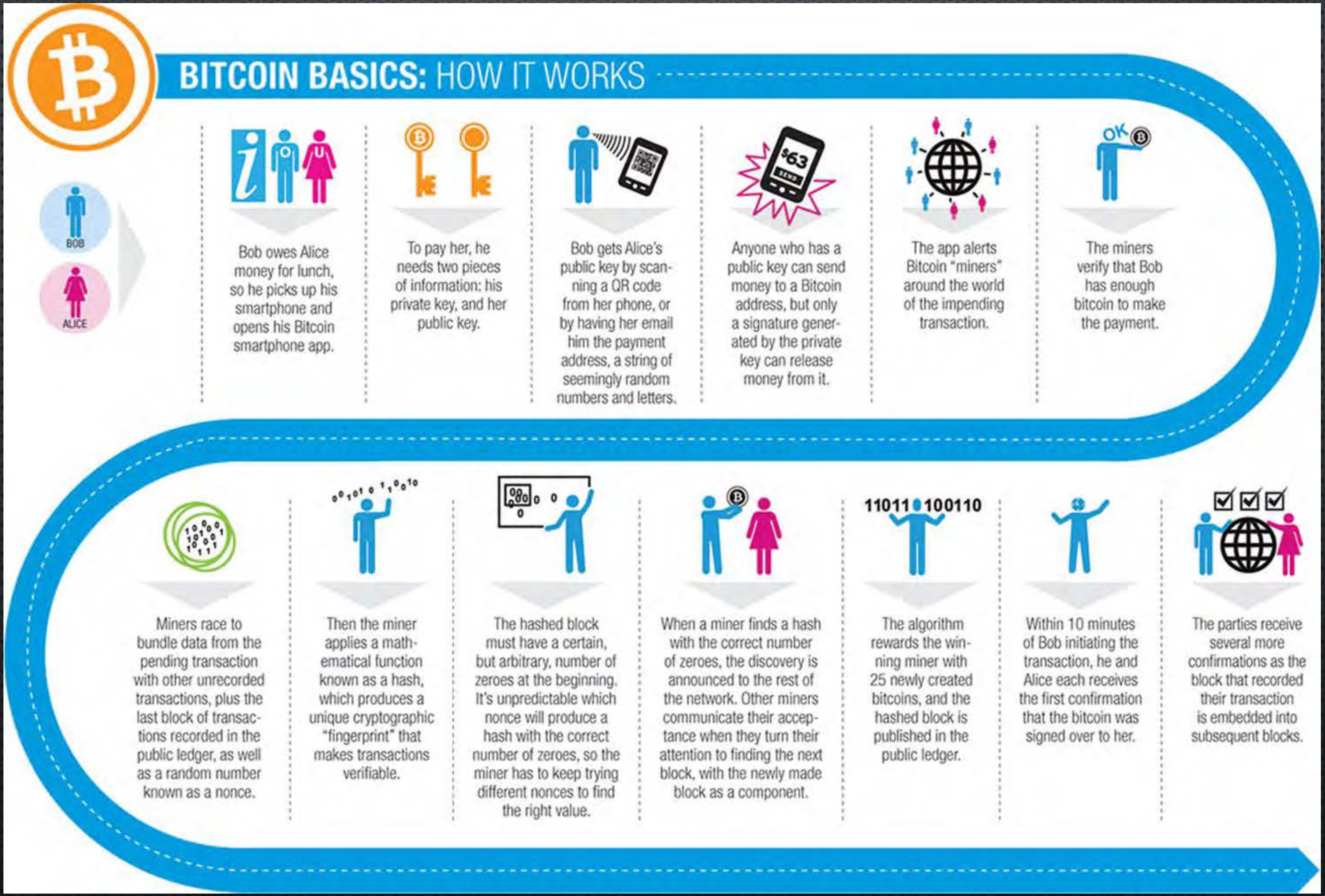
- Fiat Currency vs. Crypto
- Centralized vs Decentralized
- Distributed ledger- Blockchain
- Mined "Proof of Work"
- Wallets- custodial or non-custodial
- Cryptography is basis of security- Private keys and Public Keys

WHAT IS THE ROLE OF PUBLIC AND PRIVATE KEYS DURING CRYPTO TRANSACTIONS?

- No matter which type of wallet you use, whether you self-custody or use a custodial exchange wallet, all crypto transactions must be digitally "signed" with a private key to be completed.
- Once you initiate a transaction, your wallet constructs the transaction containing the to address, from address and amount (in addition to other metadata). Your keys are used to create a digital signature confirming the transaction is legitimate. Once the signed transaction is sent to the network, the nodes verify the signature and that the from address has enough funds to complete the transaction.
- In the case of custodial wallets, the exchange or service provider holds on to your keys, automatically signing transactions for you whenever a request is made. Some crypto users prefer this set up as it lessens their responsibility – regaining access to a lost account is as easy as tapping "Forgot password?". However, this also means that a custodial service has the power to make transactions without your consent, restrict access to your assets or even lose your funds in hacks, liquidation or bankruptcy

BITCOIN FACTS AND FIGURES

- As of July 15, 2023 Bitcoin represents 48% of crypto market
- Hard Cap of 23 Million Coins
- Mining consumes 1% of worlds electricity- more than the country of Norway



BITCOIN BASICS: HOW IT WORKS

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.

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.

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.

The algorithm rewards the winning miner with 25 newly created bitcoins, and the hashed block is published in the public ledger.

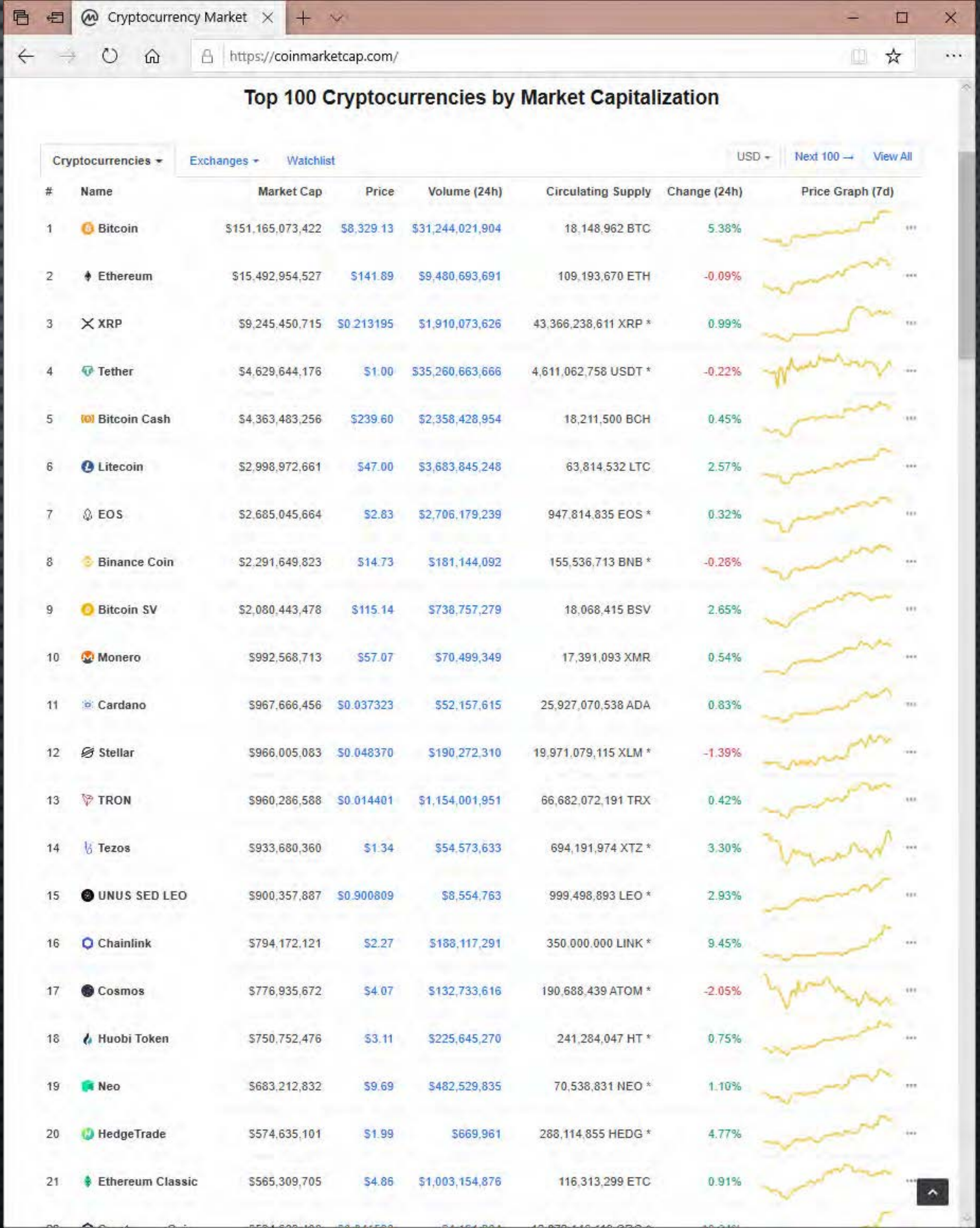
Within 10 minutes of Bob initiating the transaction, he and Alice each receives the first confirmation that the bitcoin was signed over to her.

The parties receive several more confirmations as the block that recorded their transaction is embedded into subsequent blocks.

CRYPTOCURRENCIES

WE ARE NOT JUST TALKING ABOUT BITCOIN!

NOTE THAT "TETHER" TRADING VOLUME EXCEEDS THAT OF "BITCOIN" ON THIS DAY



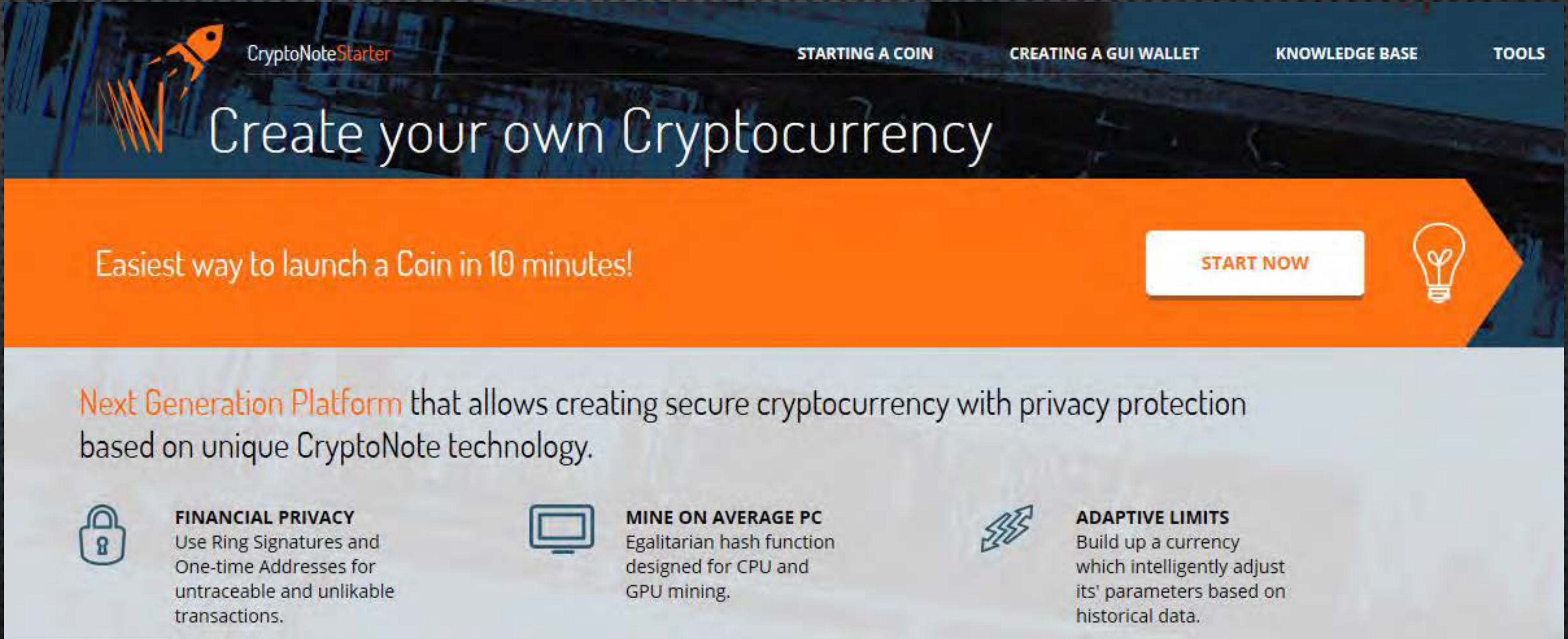
Top 100 Cryptocurrencies by Market Capitalization

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$151,165,073,422	$8,329.13	$31,244,021,904	18,148,962 BTC	5.38%	
2	Ethereum	$15,492,954,527	$141.89	$9,480,693,691	109,193,670 ETH	-0.09%	
3	XRP	$9,245,450,715	$0.213195	$1,910,073,626	43,366,238,611 XRP *	0.99%	
4	Tether	$4,629,644,176	$1.00	$35,260,663,666	4,611,062,758 USDT *	-0.22%	
5	Bitcoin Cash	$4,363,483,256	$239.60	$2,358,428,954	18,211,500 BCH	0.45%	
6	Litecoin	$2,998,972,661	$47.00	$3,683,845,248	63,814,532 LTC	2.57%	
7	EOS	$2,685,045,664	$2.83	$2,706,179,239	947,814,835 EOS *	0.32%	
8	Binance Coin	$2,291,649,823	$14.73	$181,144,092	155,536,713 BNB *	-0.26%	
9	Bitcoin SV	$2,080,443,478	$115.14	$738,757,279	18,068,415 BSV	2.65%	
10	Monero	$992,568,713	$57.07	$70,499,349	17,391,093 XMR	0.54%	
11	Cardano	$967,666,456	$0.037323	$52,157,615	25,927,070,538 ADA	0.83%	
12	Stellar	$966,005,083	$0.048370	$190,272,310	19,971,079,115 XLM *	-1.39%	
13	TRON	$960,286,588	$0.014401	$1,154,001,951	66,682,072,191 TRX	0.42%	
14	Tezos	$933,680,360	$1.34	$54,573,633	694,191,974 XTZ *	3.30%	
15	UNUS SED LEO	$900,357,887	$0.900809	$8,554,763	999,498,893 LEO *	2.93%	
16	Chainlink	$794,172,121	$2.27	$188,117,291	350,000,000 LINK *	9.45%	
17	Cosmos	$776,935,672	$4.07	$132,733,616	190,688,439 ATOM *	-2.05%	
18	Huobi Token	$750,752,476	$3.11	$225,645,270	241,284,047 HT *	0.75%	
19	Neo	$683,212,832	$9.69	$482,529,835	70,538,831 NEO *	1.10%	
20	HedgeTrade	$574,635,101	$1.99	$669,961	288,114,855 HEDG *	4.77%	
21	Ethereum Classic	$565,309,705	$4.86	$1,003,154,876	116,313,299 ETC	0.91%	

HOW MANY CRYPTOCURRENCIES ARE THERE?

22,932 Cryptocurrencies exist as of 6/17/2023 (www.coinmarketcap.com)

- Create your own in 10 minutes!
- No one will ever be an expert in them all, nor have experience tracing or seizing them.
- Refined procedures exist for dealing with common cryptocurrencies.
- When dealing with obscure cryptocurrencies, new procedures must be tested and refined based on other previously refined best practices.



Create your own Cryptocurrency

Easiest way to launch a Coin in 10 minutes!

Next Generation Platform that allows creating secure cryptocurrency with privacy protection based on unique CryptoNote technology.

FINANCIAL PRIVACY
Use Ring Signatures and One-time Addresses for untraceable and unlikable transactions.

MINE ON AVERAGE PC
Egalitarian hash function designed for CPU and GPU mining.

ADAPTIVE LIMITS
Build up a currency which intelligently adjust its' parameters based on historical data.

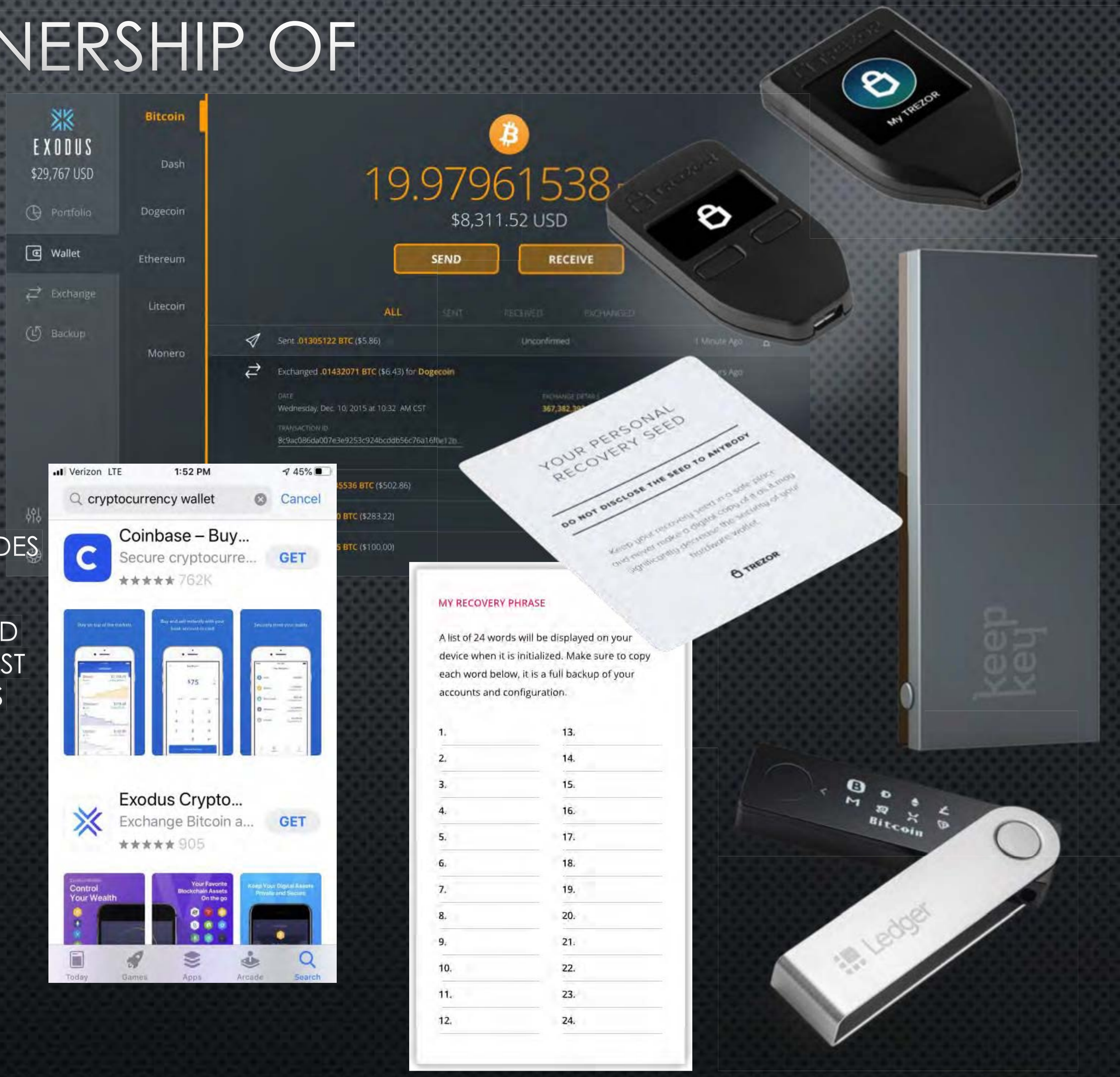
CRYPTO ATMS

- Locate at www.coinatmradar.com
- Who owns?
- Who Banks?
- Where is money going?
- Volume of use

INDICATORS OF USE/OWNERSHIP OF CRYPTOCURRENCY

POSSESSION OF:

- HARDWARE WALLETS
- SOFTWARE WALLETS
  - MOBILE AND/OR DESKTOP WALLET APPS
  - INCLUDING SOFTWARE INTERFACE TO HARDWARE WALLETS
- PAPER OR ELECTRONIC "MNEMONIC PHRASES" AND/OR "SEEDS", PUBLIC OR PRIVATE ADDRESSES/KEYS, OR QR CODES REPRESENTING ADDRESSES/KEYS
- TIP: BACK UP YOUR WALLET! ALWAYS REMEMBER TO RECORD YOUR RECOVERY PHRASE (AKA SEED PHRASE). THIS IS THE BEST WAY TO PROTECT YOUR PRIVATE KEY AND KEEP YOUR FUNDS SECURE IN CASE YOU LOSE ACCESS TO YOUR WALLET.



EXODUS
$29,767 USD

Portfolio
Wallet
Exchange
Backup

Bitcoin
Dash
Dogecoin
Ethereum
Litecoin
Monero

19.97961538
$8,311.52 USD

SEND RECEIVE

ALL SENT RECEIVED EXCHANGED

Sent .01305122 BTC ($5.86) Unconfirmed 1 Minute Ago

Exchanged .01432071 BTC ($6.43) for Dogecoin

DATE
Wednesday, Dec. 10, 2015 at 10:32 AM CST

EXCHANGE DETAILS
367,382,39

TRANSACTION ID
8c9ac086da007e3e9253c924bcddb56c76a16f0e12b

5536 BTC ($502.86)
0 BTC ($283.22)
5 BTC ($100.00)

Verizon LTE 1:52 PM 45%

cryptocurrency wallet Cancel

Coinbase – Buy...
Secure cryptocurre...
★★★★★ 762K
GET

Exodus Crypto...
Exchange Bitcoin a...
★★★★★ 905
GET

Today Games Apps Arcade Search

YOUR PERSONAL RECOVERY SEED

DO NOT DISCLOSE THE SEED TO ANYBODY

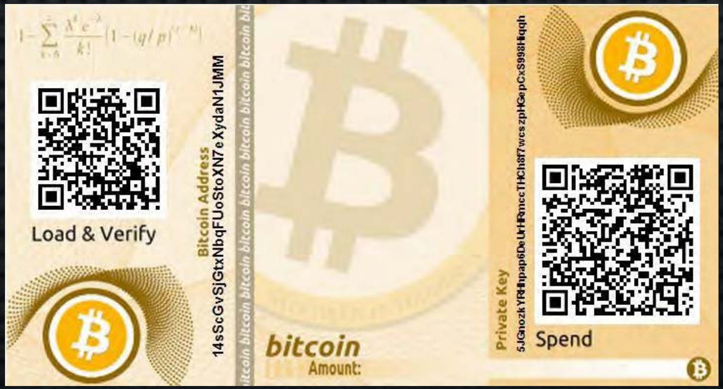
Keep your recovery seed in a safe place and never make a digital copy of it as it may significantly decrease the security of your hardware wallet.

TREZOR

MY RECOVERY PHRASE

A list of 24 words will be displayed on your device when it is initialized. Make sure to copy each word below, it is a full backup of your accounts and configuration.

1. ____ 13. ____
2. ____ 14. ____
3. ____ 15. ____
4. ____ 16. ____
5. ____ 17. ____
6. ____ 18. ____
7. ____ 19. ____
8. ____ 20. ____
9. ____ 21. ____
10. ____ 22. ____
11. ____ 23. ____
12. ____ 24. ____



Load & Verify

Bitcoin Address
14sScGvSjGtxNbqFUoStoXN7eXydaN1JMM

Private Key
5JGnozkYR8ipap6DeUrHRnccTHCh8f7wcszpHGepCxS998Hqqh

Spend

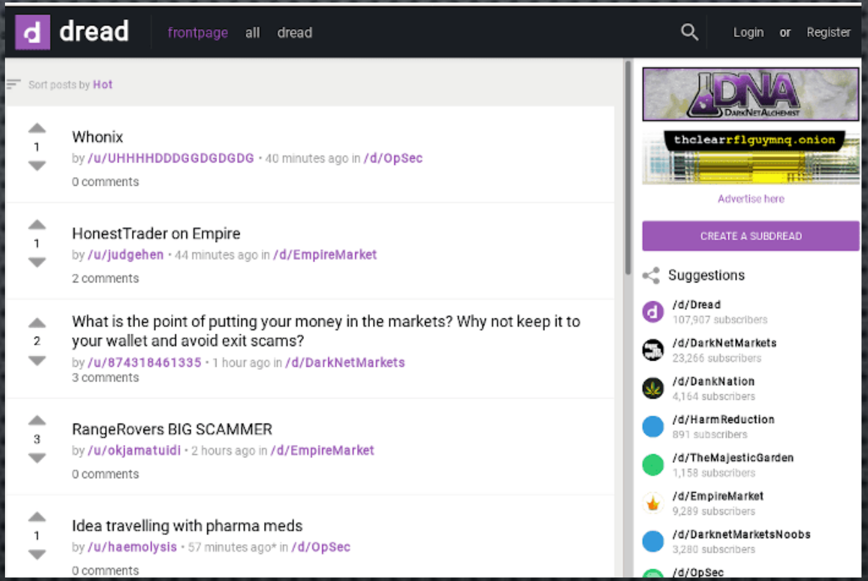
bitcoin
Amount:

INDICATORS OF USE/OWNERSHIP OF CRYPTOCURRENCY

TOR

ONLINE ACTIVITY INCLUDING:

- WEB BROWSER HISTORY, FAVORITES, OR WEB CACHE OF CRYPTO-RELATED SITES
- USE OF THE DARKWEB (TOR BROWSER, TAILS, TOR APPS, ETC.)
- SOCIAL MEDIA/FORUM POSTS OR ACTIVITY RELATING TO CRYPTO
    - REDDIT, BITCOINTALK, DREAD, ETC.



Sort posts by Hot

1 Whonix
by /u/UHHHHDDDGGDGDGDG · 40 minutes ago in /d/OpSec
0 comments

1 HonestTrader on Empire
by /u/judgehen · 44 minutes ago in /d/EmpireMarket
2 comments

2 What is the point of putting your money in the markets? Why not keep it to your wallet and avoid exit scams?
by /u/874318461335 · 1 hour ago in /d/DarkNetMarkets
3 comments

3 RangeRovers BIG SCAMMER
by /u/okjamatuidi · 2 hours ago in /d/EmpireMarket
0 comments

1 Idea travelling with pharma meds
by /u/haemolysis · 57 minutes ago* in /d/OpSec
0 comments

Suggestions

/d/Dread
107,907 subscribers

/d/DarkNetMarkets
23,266 subscribers

/d/DankNation
4,164 subscribers

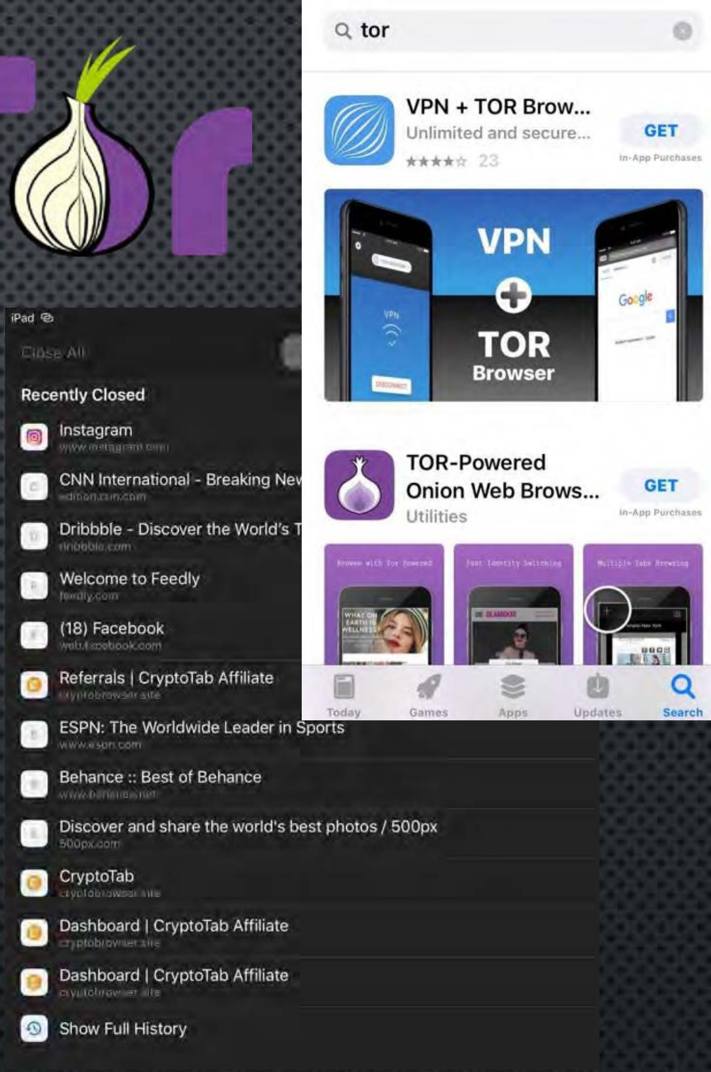
/d/HarmReduction
891 subscribers

/d/TheMajesticGarden
1,158 subscribers

/d/EmpireMarket
9,289 subscribers

/d/DarknetMarketsNoobs
3,280 subscribers

/d/OpSec



VPN + TOR Brow...
Unlimited and secure...
★★★★☆ 23

TOR-Powered Onion Web Brows...
Utilities

Recently Closed

Instagram
www.instagram.com

CNN International - Breaking New
edition.cnn.com

Dribbble - Discover the World's T
dribbble.com

Welcome to Feedly
feedly.com

(18) Facebook
web.facebook.com

Referrals | CryptoTab Affiliate
cryptobrowser.site

ESPN: The Worldwide Leader in Sports
www.espn.com

Behance :: Best of Behance
www.behance.net

Discover and share the world's best photos / 500px
500px.com

CryptoTab
cryptobrowser.site

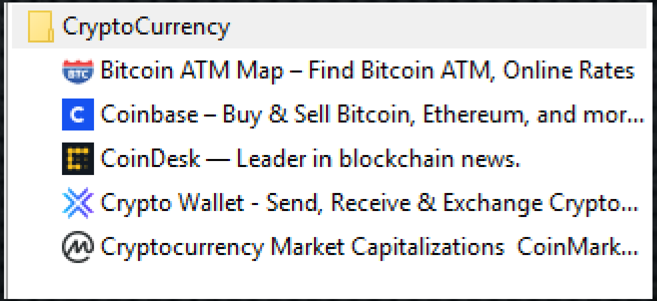
Dashboard | CryptoTab Affiliate
cryptobrowser.site

Dashboard | CryptoTab Affiliate
cryptobrowser.site

Show Full History

BITCOINTALK.ORG

/r/bitcoin



CryptoCurrency
- Bitcoin ATM Map – Find Bitcoin ATM, Online Rates
- Coinbase – Buy & Sell Bitcoin, Ethereum, and mor...
- CoinDesk — Leader in blockchain news.
- Crypto Wallet - Send, Receive & Exchange Crypto...
- Cryptocurrency Market Capitalizations CoinMark...

WHERE DO YOU START?

You have leads or other information indicating that a subject may use/own cryptocurrency. Now what?

- Conduct research, Surveillance and/or Undercover Operations (Online or in-person), Obtain records via Legal Process, Intercepts, Interviews and other standard investigative steps.
  - What cryptocurrencies are involved?
  - What exchanges?
  - What wallet type and how does the subject access it?
  - What addresses/keys can you identify?
  - Available records and legal authorities will vary from country to country.
- Blockchain tracing – follow the bouncing ball
  - Commercial ventures Trace Bitcoin and a handful of the most common cryptocurrencies
- Visualization and analytical tools used to identify connections and patterns

CHAINALYSIS

ELLIPTIC

coinbase

IBM i2 Analyst's Notebook

Palantir

MALTEGO

FINANCIAL RECORDS

- The money MUST enter the system somewhere.
- Look for money sent or received from an exchanger
- Check Credit card records for charges by Crypto exchange
- Mobile money records – follow the trail to a financial institution
- If you can find the exchanger, you can likely find the wallet