PROGRAM MATERIALS
Program #29183
December 5, 2019

Building Cryptocurrency + Blockchain Investigations Involving Bitcoin / Crypto Automated Teller Machines (BTMs / CTMs)

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 180, Boca Raton, FL 33487
Phone 561-241-1919 Fax 561-241-1969

Building Cryptocurrency + Blockchain Investigations Involving Bitcoin / Crypto Automated Teller Machines

Lourdes C. Miranda, Cryptocurrency Analyst + Financial Crimes Investigator

Celesq® AttorneysEd Center | Webinar
December 5, 2019

Celesq® AttorneysEd Center

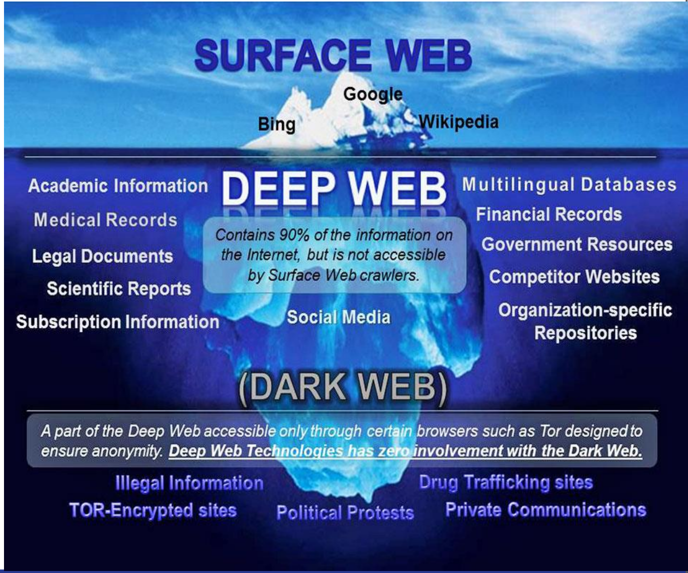
Cryptocurrency Lingo

Addresses	Public Key (26 - 35 alphanumeric characters, beginning with the numbers 1, 3, or bc1) (think of bank account numbers) Private Key (only known to the owner and starts with a 5, K, or an L) (think of passwords / PIN)
Blockchain	Public Ledger (think of financial statements)
BTMs or CTMs	Bitcoin Automated Teller Machines or Crypto Automated Teller Machines
Cryptocurrencies	Virtual / Digital Currencies (crypto = using digital encryption) (currency = a system of money)
Exchangers	Financial Institutions (think of banks, credit unions, brokerage firms, money service businesses)
Mining	Creating Cryptocurrencies and Validating Transactions
Mixers (aka Tumblers, Laundries, Washers)	Exchangers (think of Financial Institutions that does currency conversion)
Public Keys (to encrypt)	The Mailbox that Generates, Stores, and Sends (think of Bank Account Numbers)
Private Keys (to decrypt)	The Mailbox that Stores your Passwords / PINs (only known to the owner & authorizes the owner to execute transactions from their account. To send Bitcoin, you must sign with your private key)
Seed Phrase	Words which Store all the Information Needed to Recover a Bitcoin Wallet (think of passwords / PIN)
Shifters	Exchangers (think of Financial Institutions that does currency conversion)
Transaction Hash / ID / TXID	A Random Sequence of Characters that is given to every Transaction that is Verified and Added to the Blockchain (think of Personally Identifiable Information)
Transaction Input	Bitcoin Address from which the money was sent (think of your checking account number)
Transaction Output	Bitcoin Address to which the money was sent (think of Pay to the Order of)
Wallet (hard / soft)	Where your Bitcoin Address is Stored (think of the routing number on your checking / savings account) (think of a bank safety deposit box)

Deep Web / Dark Web (The Onion Router = TOR)

- ❑ https://www.onion-router.net
- ❑ https://www.torproject.org (download TOR)
- ❑ https://www.electrum.onion (TOR URL example)
- ❑ https://www.nyt.onion (*The New York Times*)

- ❑ Enables anonymous communication by concealing user’s location and usage
- ❑ Research
- ❑ Open accounts and execute transactions with more anonymity



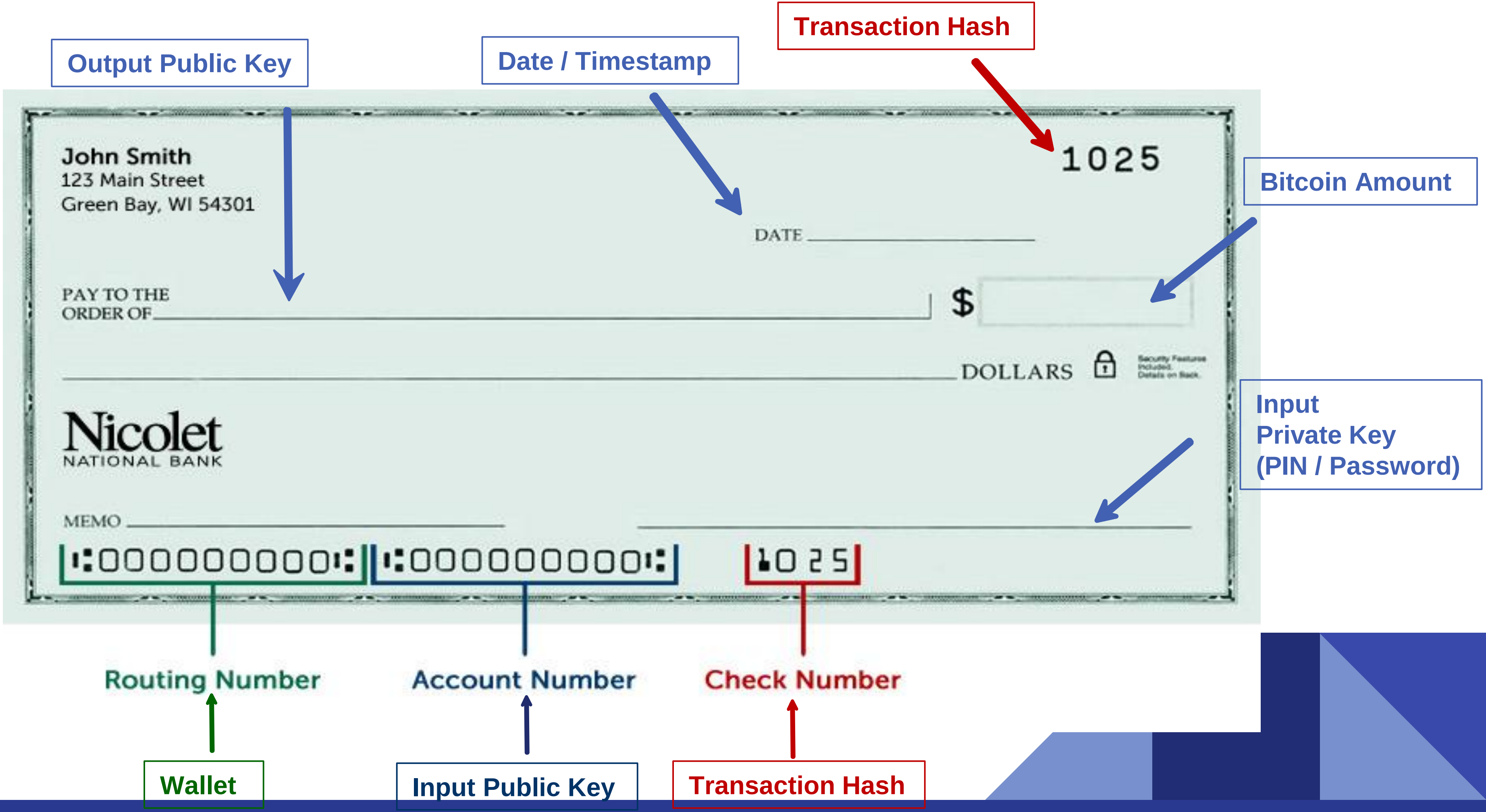
Contains 90% of the information on the Internet, but is not accessible by Surface Web crawlers.

A part of the Deep Web accessible only through certain browsers such as Tor designed to ensure anonymity. ***Deep Web Technologies has zero involvement with the Dark Web.***

REDDIT using TOR

- Social news groups / discussion websites / blogs
- Bad actors use to:
  - advertise products and services
  - conduct research
  - communicate with associates
  - monitor the news (i.e., which services were shut down by federal law enforcement and/or hacked)
  - rate exchangers + wallet + mixers + shifter services
  - search for BTM / CTM locations inside and outside the United States
- **Excellent Source for:**
  - collecting intelligence
  - developing investigative leads
  - developing sources / assets

www.reddit.com/r/CryptoCurrency



Output Public Key

Date / Timestamp

Transaction Hash

Bitcoin Amount

Input
Private Key
(PIN / Password)

Wallet

Input Public Key

Transaction Hash

Purchasing Cryptocurrency

GEMINI

- Accepts cash
- Accepts Visa or MasterCard (debit/credit)
- Accepts wire transfers
- Buy/sell/trade/convert BTC in real time
- Complies with US regulations **(strong AML requirements)**
- Offers digital wallets (equivalent to an online bank account)
- Requires identification
- **Converts to fiat currency**

- Accepts cash
- Accepts Visa or MasterCard (debit / credit) (prepaid)
- **Some BTMs / CTMs don’t require identification**
- Prints receipts
- **Use burn phone to use Quick Response (QR) code from wallet**
- https://coinatmradar.com/countries
- www.coinsource.net
- **Some convert to fiat currency**

Note: Use https://coinmarketcap.com/ to collect archived conversion for building cases

Will BTMs / CTMs Replace Wire Transfers?

“Police in Spain Say Bitcoin ATMs Expose Problems in Europe’s AML Laws”
Coindesk.com
July 11, 2019
https://www.coindesk.com/police-in-spain-say-bitcoin-atms-expose-problems-in-europes-aml-laws

“DIY Bitcoin ATM Money Launderer Pleads Guilty”
NewsBTC.com
August 26, 2019
https://www.newsbtc.com/2019/08/26/diy-bitcoin-atm-money-launderer-found-guilty/

“Bitcoin ATM Firm ‘Auscoin’ a Front for International Drug Smuggling Ring: Australian Police”
CCN.com
April 22, 2019
https://www.ccn.com/australia-bitcoin-atm-firm-auscoin-front-drug-ring-police

“Are Bitcoin ATMs Driving Adoption, Criminality, or Consumerism?”
NewsBTC.com
February 7, 2019
https://www.newsbtc.com/2019/02/07/bitcoin-atms-adoption/

“International Bitcoin Teller Machines: Another Money-Laundering Vehicle or Legitimate Enterprise?”
Thomson Reuters
November 27, 2018
http://www.legalexecutiveinstitute.com/bitcoin-teller-machines/

“Bloomberg, Coinsource Report Indicates Bitcoin ATMs Are Money Laundering Vehicles”
BitcoinExchangeGuide.com
December 17, 2018
https://bitcoinexchangeguide.com/bloomberg-coinsource-report-indicates-bitcoin-atms-are-money-laundering-vehicles/

“Bitcoin ATMs May Be Used to Launder Money”
Bloomberg Businessweek
December 14, 2018
https://www.bloomberg.com/features/2018-bitcoin-atm-money-laundering

“How a Dark Web Drug Ring Was Uncovered After Suspicious A.T.M. Withdrawals”
The New York Times
April 16, 2019
https://www.nytimes.com/2019/04/16/nyregion/dark-web-drug-dealing.html?searchResultPosition=1

District Attorney – New York County
April 16, 2019
“Manhattan District Attorney Vance Partners Take Down Major Dark Web Drug Seller”
https://www.manhattanda.org/d-a-vance-partners-take-down-major-dark-web-drug-seller/

BTMs / CTMs International Bad Actors Could Use the Following:

Foreign-based services that require limited or no Personally Identifiable Information (PII) at:

- Airport Kiosks
- Beach Resorts
- Casinos
- Coffee Shops
- Hotels
- Money Service Businesses
- Shopping Centers / Markets
- Subway Stations
- Universities

❑ Hire people to open accounts and/or use BTMs / CTMs using their legitimate PII

✓ Students and faculty can be popular recruits

❑ Legitimate and/or stolen credit/debit/prepaid cards to purchase cryptocurrency

❑ **Most Threatening: Bad actors owning and operating their own BTMs / CTMs** (https://bitcoinatm.com (Genesis); https://www.digitalmint.io)

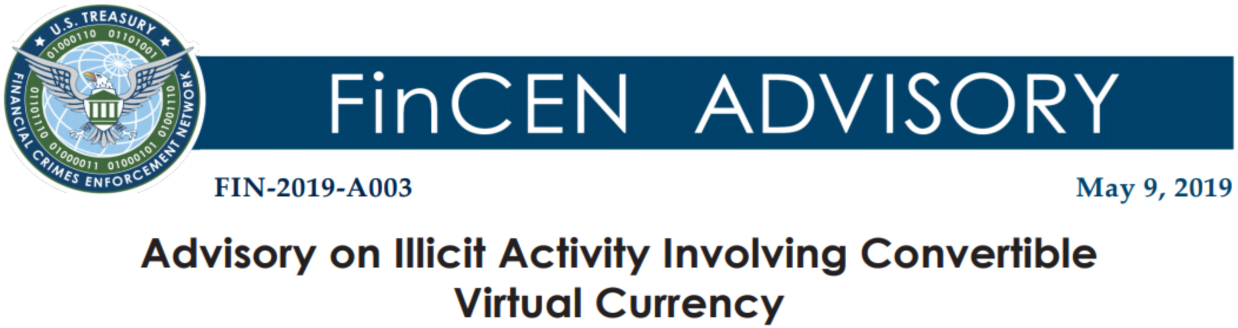
❑ Some BTM / CTM deposits under $3,000 don’t require PII

✓ **For deposits over $3,000 and other PII requirements, bad actors will use burn phones to circumvent strong AML protocols**

Mining + Fees

- ❑ Mining is the act of creating cryptocurrencies using algorithms and validating transactions
- ❑ Mining is the process by which transactions are verified and added to the blockchain
- ❑ Mining fees fluctuate
  - ✓ https://bitcoinfees.21.co to verify the miner’s fee before conducting transactions
- ❑ Mining fees are paid each time a user sends a transaction
- ❑ An indicator of nefarious activity is when the mining fee / transaction fee is very high
  - ✓ Note: this reporting should be included in SARs / CTRs because:
    - ➢ Bad actors are willing to pay higher fees to move cryptocurrency faster
    - ➢ The higher the miners / transaction fee, the faster the crypto will be verified and moved

Note: According to FinCEN, miners are not MSBs



FinCEN ADVISORY

FIN-2019-A003

May 9, 2019

Advisory on Illicit Activity Involving Convertible Virtual Currency

- ❑ Exchangers + BTMs / CTMs are considered Money Service Businesses and **MUST**:
  - ✓ Register with The Financial Crimes Enforcement Network (FinCEN)
  - ✓ File Suspicious Activity Reports (SARs)
  - ✓ File Currency Transaction Reports (CTRs)
  - ✓ Have Anti-Money Laundering (AML) and the Countering Financing of Terrorism (CFT) programs

- ❑ Exchangers + BTMs/ CTMs are subject to on-site examination by the IRS

https://www.fincen.gov/sites/default/files/advisory/2019-05-10/FinCEN%20Advisory%20CVC%20FINAL%20508.pdf

Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses

November 2018

❑ The U.S. Department of the Treasury’s Office of Foreign Assets Control (OFAC) took action today against two Iran-based individuals, Ali Khorashadizadeh and Mohammad Ghorbaniyan, who helped exchange digital currency (bitcoin) ransom payments into Iranian rial on behalf of Iranian malicious cyber actors involved with the SamSam ransomware scheme that targeted over 200 known victims.

❑ Khorashadizadeh and Ghorbaniyan used the following two digital currency addresses: 149w62rY42aZBox8fGcmqNsXUzSStKeq8C and 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V. Since 2013, Khorashadizadeh and Ghorbaniyan have used these two digital currency addresses to process over 7,000 transactions, to interact with over 40 exchangers—including some US-based exchangers—and to send approximately 6,000 bitcoin worth millions of USD, some of which involved bitcoin derived from SamSam ransomware.

https://www.treasury.gov/resource-center/sanctions/SDN-list/Pages/default.aspx

https://home.treasury.gov/news/press-releases/sm556

Financial Action Task Force

The Travel Rule was adopted in June 2019 by FATF. It requires cryptocurrency exchanges, some digital wallet providers and other firms to send customer data—including names and account numbers—to institutions receiving transfers of digital funds, similar to a wire transfer at a bank. **The goal of the travel rule is to help law enforcement track suspicious activity.**

FATF

GUIDANCE FOR A RISK-BASED APPROACH

VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS

In June 2019, FATF updated it's June 2015 guidance by adding "virtual currency" to Recommendation 15 (New Technologies) to mandate that exchangers are regulated, licensed/registered and are subject to monitoring; required to conduct customer due diligence, recordkeeping, and suspicious transaction reporting—just to name a few; sanctions and other enforcement measures; and international cooperation. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html

40 Recommendations + 9 Special Recommendations on Terrorism Financing as of June 2019. https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FATF

INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION

The FATF Recommendations

FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction. The FATF Recommendations are recognized as the global AML and CFT standard. http://www.fatf-gafi.org

The Five Pillars of the Bank Secrecy Act's AML + CFT Requirements For Exchangers + BTMs / CTMs

1. Designate a Bank Secrecy Act Compliance Officer (CO)
2. Establish internal controls, policies, procedures specific to your business model
3. Establish AML / CFT training for appropriate personnel—including Board of Directors, senior management, CO, and other relevant staff
4. Conduct periodic independent AML / CFT testing / review to ensure compliance (i.e., audits)
5. Establish a risk-based, customer due diligence procedures

Exchangers + BTM / CTM Owners and Operators are Required to:

- ✓ Conduct customer due diligence for transactions is $1,000 or more
- ✓ Maintain recordkeeping for transactions equal to or more than $3,000 and request personally identifiable information
- ✓ File SARs and CTRs for transactions of more than $10,000 in cash and any nefarious activity regardless of amount

Section 352 of the USA PATRIOT ACT amended the BSA to require financial institutions, including broker-dealers, to establish AML programs.
https://www.sec.gov/about/offices/ocie/amlsourcetool.htm

Note: Use your investigative + analytical tools with cryptocurrency / blockchain tools

Building a Criminal Case Involving Cryptocurrency

Include the following reporting in your SARs / CTRs:

- ❑ Public Key(s)
  - ✓ Exchanger(s)
  - ✓ Independent Wallet Service(s) (i.e., Electrum, MyMonero)
- ❑ Mining Fees / Transaction Fees
  - ✓ An indicator of nefarious activity is when the mining fees / transaction fees are very high
- ❑ Archived Amount Conversion
  - ✓ Use https://coinmarketcap.com (Crypto to Fiat Currency)
- ❑ Investigative + Analytical Tools
  - ✓ CipherTrace
  - ✓ https://www.blockchain.com/explorer
  - ✓ https://www.walletexplorer.com
  - ✓ https://blockstream.info
- ❑ Blockchain in Establishing the Chain of Custody
  - ✓ Hash Number
  - ✓ Public Keys
  - ✓ Date / Time Stamp
  - ✓ Mining Fee / Transaction Fee

Chain of Custody on the Blockchain

- The blockchain can be used for forensic investigations + intelligence collection to establish the **chain of custody**
  - Chain of custody is the process of handling evidence from the time it is collected until it is presented as evidence in a court of law:
    - **Integrity:** the evidence has not been altered or corrupted during the transferring
    - **Traceability:** the evidence must be traced from the time of its collection until it is destroyed
    - **Authentication:** all the entities interacting with a piece of evidence must provide an irrefutable sign as recognizable proof of their identity
    - **Verifiability:** the whole process must be verifiable from every entity involved in the process
    - **Security:** changeovers of an evidence cannot be altered or corrupted

- The blockchain can **retain the integrity of digital evidence** because it is:

S = Secure
I = Incorruptible
T = Transactions are irreversible
E = Encrypted

- The hash numbers on the blockchain include:
  - Date / timestamp of validated transactions which prevents fraudulent transactions and double spending
  - Amount
  - Sender / receiver of the funds (public keys)

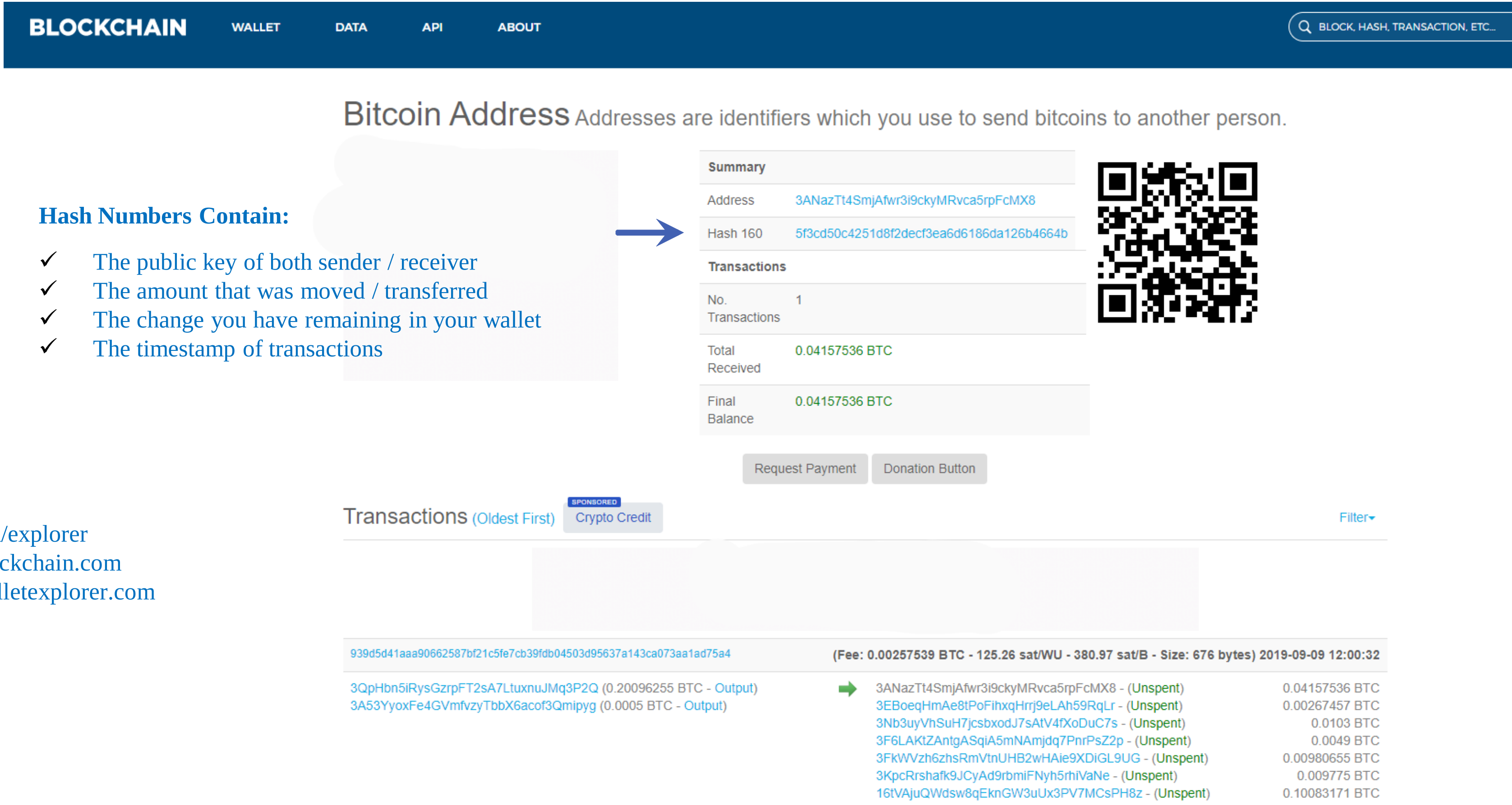
Hash Numbers

Hash Numbers Contain:

- ✓ The public key of both sender / receiver
- ✓ The amount that was moved / transferred
- ✓ The change you have remaining in your wallet
- ✓ The timestamp of transactions

Tools:

- ✓ Blockchain.com/explorer
- ✓ https://www.blockchain.com
- ✓ https://www.walletexplorer.com



Bitcoin Address Addresses are identifiers which you use to send bitcoins to another person.

Summary	
Address	3ANazTt4SmjAfwr3i9ckyMRvca5rpFcMX8
Hash 160	5f3cd50c4251d8f2decf3ea6d6186da126b4664b
Transactions	
No. Transactions	1
Total Received	0.04157536 BTC
Final Balance	0.04157536 BTC

Transactions (Oldest First)

939d5d41aaa90662587bf21c5fe7cb39fdb04503d95637a143ca073aa1ad75a4 **(Fee: 0.00257539 BTC - 125.26 sat/WU - 380.97 sat/B - Size: 676 bytes) 2019-09-09 12:00:32**

3QpHbn5iRysGzrpFT2sA7LtuxnuJMq3P2Q (0.20096255 BTC - Output)
3A53YyoxFe4GVmfvzyTbbX6acof3Qmipyg (0.0005 BTC - Output)

3ANazTt4SmjAfwr3i9ckyMRvca5rpFcMX8 - (Unspent)	0.04157536 BTC
3EBoeqHmAe8tPoFihxqHrrj9eLAh59RqLr - (Unspent)	0.00267457 BTC
3Nb3uyVhSuH7jcsbxodJ7sAtV4fXoDuC7s - (Unspent)	0.0103 BTC
3F6LAKtZAntgASqiA5mNAmjdq7PnrPsZ2p - (Unspent)	0.0049 BTC
3FkWVzh6zhsRmVtnUHB2wHAie9XDiGL9UG - (Unspent)	0.00980655 BTC
3KpcRrshafk9JCyAd9rbmiFNyh5rhiVaNe - (Unspent)	0.009775 BTC
16tVAjuQWdsw8qEknGW3uUx3PV7MCsPH8z - (Unspent)	0.10083171 BTC

Blockchain Disadvantages

The blockchain is **pseudonymous** and **doesn’t provide 3rd party intelligence** because there’s no personally identifiable information (PII) about the bad actors behind each transaction

To support Subpoenas, Search Warrants, FISA, and Mutual Legal Assistance Treaty coordination, 3rd party intelligence / PII can be collected from:

- □ Bitcoin ATM owners and operators
- □ Confidential sources
- □ Intelligence sources
- □ Investigative / analytical tools (i.e., CipherTrace, blockchain.com/explorer)
- □ Employees from exchanges and wallets services
- □ Employees from financial institutions (i.e., banks, credit unions, trust companies, brokerage firms)
- □ Law enforcement informants
- □ Money service businesses
- □ Electronic interception

Building Cryptocurrency + Blockchain Investigations Involving Bitcoin / Crypto Automated Teller Machines

Thank You

Lourdes C. Miranda, Cryptocurrency Analyst + Financial Crimes Investigator

lourdes@mirandafinintel.com
https://www.linkedin.com/in/lourdescmiranda
(703) 283-8940

Celesq® AttorneysEd Center