FOCUS ON WHAT COUNTS

CRYPTOCURRENCY FRAUD & FORENSICS

TEAM WORK
Presented by:

– Mark DiMichael, CPA/ABV/CFF, CFE (Forensic Accountant)
Crypto Assets

• An asset in which encryption is used to verify transactions and regulate the creation of new units.

• Bitcoin was the first. Now there are thousands of cryptocurrencies.

• Various Terminology

• How it works
Technology Cheat Sheet

• **Blockchain** – With regard to cryptocurrency, a blockchain is a historical, public ledger of every transaction since inception of that cryptocurrency. The blockchains for cryptocurrencies are maintained in a “decentralized” manner - meaning that copies of the blockchain are maintained on many computers, globally (rather than a centralized computer controlled by a third party financial institution). The blockchain activity can be viewed on various publicly available “block explorer” websites, such as [www.blockchain.info](http://www.blockchain.info) for Bitcoin.

• **Public Addresses** - An individual stores their cryptocurrency in a “public address”, which is represented as a string of alphanumeric characters (i.e. KqDCQGETTSLcxgbbJU2wwqTtNqG4Hyv8o). The public address acts as an account number that exists only as an entry on the blockchain. One individual can have an unlimited number of public addresses.

• **Private Keys** - The funds in each public address are controlled through the use of another string of alphanumeric characters called a “private key”. The private key acts as the secret password required for the spending of funds in a particular public address. Anyone who possesses the correct private key can spend the funds in the associated public address.
  
  If a private key is ever lost or destroyed, the funds are locked away permanently (since no one has the private key needed to spend those funds). If the private key is ever stolen by hackers, the funds can be taken by the hackers, and the original owner has no recourse.

• **Wallet Seed** - An individual’s private keys are usually generated from a string of 12, 15, 18, 21, or 24 randomly generated words called a “seed” (i.e. crash noise pluck unique elbow hero income coyote emotion modify service alter). One seed can generate an endless supply of private key/public address pairs.
Centralized Model

Third Party Bank / Brokerage Account / Exchange

Depositor #1
Scott
$5,000

Depositor #2
Mary
$2,000

Depositor #3
Rosie
$12,000
De-Centralized Model (The Blockchain Model)

Miner #1 (with a copy of the Blockchain)
- Address #1: 2.4 BTC
- Private Key

Miner #2 (with a copy of the Blockchain)
- Address #2: 5 BTC
- Private Key

Miner #3 (with a copy of the Blockchain)
- Address #3: 0.675 BTC
- Private Key
Miners

• Miners provide computing power to verify transactions

• Non-permissioned - Anyone with the right hardware/software

• Miners are compensated for their efforts with newly created bitcoins and with transaction fees

• Add blocks to the blockchain based on majority rule
The Blockchain

• Miners record legitimate transactions publicly, permanently, and immutably in the blockchain.

• It’s security results from contributions from three separate scientific disciplines
  – Cryptography
  – Computer Science
  – Game Theory (used in politics, economics, etc.)

• Blockchain technology is currently being used by JPM Chase, Walmart, Microsoft and more. Many other companies are exploring / investing in potential use cases.
Other Uses For Blockchain & Digital Assets

- Data storage among multiple third parties
- Built-in “Smart Contracts”
- Tokenization
Other Digital Assets

• Faster than Bitcoin
  – Litecoin
  – Bitcoin Cash

• “Privacy Coins”
  – Monero
  – Z-Cash
  – Verge

• Other Decentralized Platforms
  – Ether / Etherium (Smart Contracts)
  – XRP / Ripple (Payment Processing)

• Many more
• **Paper Wallet** - A paper wallet is simply the act of maintaining one’s private keys, public addresses, and/or wallet seed printed on physical paper. While this is very safe and effective for long-term storage of cryptocurrency, it is not practical for individuals who regularly transact in cryptocurrency, since implementing transactions requires a computer.

• **Software Wallet** - A software wallet is a phone or computer application that can generate private keys/public addresses, and can initiate transactions. Software wallets provide easy use and access to cryptocurrency funds, but are potentially susceptible to hackers.

• **Hardware Wallet** - A hardware wallet is a password protected electronic device that looks similar to a USB flash drive. A hardware wallet is specifically designed to generate and store private keys. A hardware wallet is generally immune to hackers because it is generally not physically connected to a computer or the internet.

• **Exchanges** – Third party websites that facilitate the buying and selling of cryptocurrency. Exchanges generally control the private keys and users do not have access to the private keys. Instead, the exchanges initiate all transactions and the user will merely have an account with that third party exchange, similar to keeping one’s money at a bank.
Regulators

• Commodities Futures & Trading Commission (CFTC)

• NY Department of Financial Services – the “BitLicense”

• State by state enforcement against ICOs (Texas and other states)

• The Securities & Exchange Commission
Common Types of Fraud Involving Cryptocurrency

• Cryptocurrency Specific Frauds
  – ICO Fraud
  – 51% Attack

• General Frauds
  – Tax fraud
  – Individuals Hiding Assets (Bankruptcy, Divorce, etc.)
  – Money laundering
  – Phishing scams
Initial Coin Offerings

• An unregulated means of crowdfunding, utilizing digital assets (referred to as a “token”).

• Company creates tokens, which they sell to investors for other currencies.

• Whitepaper provided to potential investors

• Companies have utilized ICOs to raise millions in capital.
ICO Fraud

• “Initial Coin Offering”
  – Example

• Red Flags:
  – Forecasts of unreasonable returns on investment
  – Quickly thrown together whitepaper and promotion materials
  – Ability to purchase coins with a credit card
  – Fake or non-existent project team members
  – Celebrity endorsements
  – Claims of an SEC compliant coin / compliant exchange
  – One-time only deals or discounts for purchases by a certain date
  – Plagiarized text from other whitepapers and projects

• Wall Street Journal performed an in-depth analysis of the whitepapers, websites, and marketing materials for 1,450 ICOs and found that 271 (nearly 1 out of 5) contained red flags of fraud.
Security / Investment Tokens - The Howey Test

- SEC v. W.J. Howey Co. (1946) – The Howey Test
  1. A person invests their money
  2. In a common enterprise
     - Horizontal commonality
     - Narrow or strict vertical commonality
     - Broad vertical commonality
  3. With an expectation of profits
     - At the time of purchase, the investor must have a reasonable expectation of profits
       - Intent of purchaser
       - Advertising materials to promote the ICO
  4. Profits, if any, result from the efforts of others

- This is a complicated and robust area of case law. Consider consulting a securities attorney.
Securities & Exchange Commission Enforcement

- SEC
  - DAO Token Report dated July 25, 2017
  - Munchee Token

  - The SEC Chairman, Jay Clayton has stated “I believe every ICO I’ve seen is a security”.
    - The SEC is taking increasingly strong action against unregistered ICOs, but, the vast majority of ICOs are not registered and the SEC has only taken enforcement action in a very limited number of circumstances where there has been obvious fraud.

  - Some alleged ICO scams pursued by the SEC- AriseCoin, REcoin, DRC, and CTR Token
51% Attacks
Tax Fraud

• Tax evasion is rampant.

• IRS Coinbase Summons

• IRS Chainalysis Research

• 10,000 “educational letters” sent out in August 2019 to cryptocurrency owners
• Defines Convertible Virtual Currency

• Application of property rules, rather than currency rules

• Discusses
  – Receipt of virtual currency for goods and services
  – Receipt of virtual currency for mining
  – Applicability of capital gains vs. ordinary income treatment on sales
  – Discusses reporting requirements (i.e. 1099, W-2, & 1099-K)
IRS Revenue Ruling 2019-24

- Two Concepts that Result in Individuals Receiving Cryptocurrency
  - Hard Fork
  - Airdrop

- Constructive Receipt
  
  - The IRS revenue ruling incorrectly uses the term “airdrop”

- Released with an FAQ
  
1040 Schedule 1

• “At any time during 2019, did you receive, sell, send, exchange, or otherwise acquire any financial interest in any virtual currency?”

• Required schedule for all taxpayers, as of 2019

• Confusion about gaming currency
  – Some gaming currencies are convertible
Hiding Cryptocurrency (Matrimonial, Bankruptcy, etc.)

- Bank Accounts & Credit Card Statements
- Tax Returns
- Legal Discovery & Depositions
- Subpoenas to Exchanges
- Loan Applications
- Obtaining Alternate Assets
- Forensic Expert Analysis of Electronic Devices
Physical Evidence of Cryptocurrency - Paper Wallets
Physical Evidence of Cryptocurrency - Hardware Wallets
### Summary

<table>
<thead>
<tr>
<th>Hash</th>
<th>Amount</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>770c10bf03cf960d6ee1604f3d5fc3854abbb49c1526b11f7d262...</td>
<td>1.11998347 BTC</td>
<td>2020-03-03 06:20</td>
</tr>
<tr>
<td>1G4JnoRCbatG8Fqussc99V9ifznhr37eb4</td>
<td>0.0908801 BTC</td>
<td>3HyUpcnFrDnXHMP2SGQ8Fh9tv4evEuQWD</td>
</tr>
<tr>
<td>1G4JnoRCbatG8Fqussc99V9ifznhr37eb4</td>
<td>0.0216068 BTC</td>
<td></td>
</tr>
<tr>
<td>12W4M8Pw6sEKAKyJvD6UzLZ4A50c5U98ki</td>
<td>0.55498095 BTC</td>
<td></td>
</tr>
<tr>
<td>12ebhE8nKlD4E3VvWuK1vBVEF3M2zkT8rRbUJ</td>
<td>0.40549683 BTC</td>
<td></td>
</tr>
</tbody>
</table>

### Fee

- 0.00014228 BTC (21.363 sat/B - 5.341 sat/WU - 666 bytes)
- 2.17120698 BTC

### Details

- **Hash**: 770c10bf03cf960d6ee1604f3d5fc3854abbb49c1526b11f7d262f5c08dd114
- **Status**: Confirmed
- **Received Time**: 2020-03-03 06:20
- **Size**: 666 bytes
- **Weight**: 2,664
- **Included in Block**: 619982
- **Confirmations**: 15
- **Total Input**: 2.17134926 BTC
- **Total Output**: 2.17120698 BTC
- **Fees**: 0.00014228 BTC

---

**John Smith**

**Change**
Blockchain Data Analytics

- Block Chain Analysis through available forensic tools / data analytics:
  - Reactor by Chainalysis (Used by the IRS)
  - Skry
  - Numsight
  - Elliptic

- Tools for tracing/consolidating transactions:
  - Walletexplorer.com
  - www.oxt.me
  - Cointracking.info
Tracing Bitcoin Transactions

• The Binance Hack
  – https://www.blockchain.com/btc/tx/e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea

• 3 Methods of Tracking
  – 2 tainted bitcoin and 3 clean bitcoin go into a transaction. All 5 are spent
    • Aggressive Method
    • First In First Out
    • Percentage Method

• Considerations:
  – Potential for two or more separate markets to exist for the same coin
  – Do the coins ever become clean again?
Money Laundering

• Present the illicit income as if it was the result of a profitable venture

• Cryptocurrency ecosystem that can help enable money laundering
  – www.localbitcoins.com
  – Dark websites
  – Prepaid debit cards and gift cards
  – Unregulated exchanges
  – Cryptocurrency ATMs
Cryptocurrency Mixing Example

A adds 10XFC to F
B adds 10XFC to E
C adds 10XFC to D

A

10XFC

B

10XFC

C

10XFC

30XFC

D

4XFC

6XFC

E

7XFC

3XFC

F

8XFC

2XFC
Monero – Ring Signatures

- One-Time Addresses
- No Amount Visible on Blockchain
Phishing Scheme

- Attempt to get your address, private keys or seeds
- Ransomware
  - Cryptocurrency payments made to ransomware attackers increased nearly 90% in Q1 of 2019
  - 98% of attackers ask for cryptocurrency as payment
  - What to do when you’ve been attacked?
    - Contact law enforcement
    - If practical/possible, just restore most recent backups
    - Consider working with consultant to
      - Correspond with attackers
      - Verify hackers actually have the keys to unencrypt your date
      - Negotiate
      - Pay & pray
Wait.....Is this whole thing legal?

- Bernard Von Nothaus
- Liberty Reserve Dollar
- Federal prosecutors seized and sold 29,655 bitcoins from “Dark Web” site, Silk Road in 2014.

- Can it be shut down?
  - Bitcoin (and other cryptocurrencies) are electronic and decentralized.
Conclusion

• Any fraud committed with cash can be committed using cryptocurrency

• Cryptocurrency provides new, unique ways that individuals can commit fraud.

• If you have proven an individual owns cryptocurrency, there is no way to be 100% sure you have uncovered it all.
Questions
Contact Information

Mark DiMichael, CPA/ABV/CFF, CFE
Partner

Phone:  212-697-1000
E-mail:  mdimichael@citrincooperman.com
Citrin Cooperman & Company, LLP
New York Office
FOCUS ON WHAT COUNTS

CITRINCOOPERMAN.COM