Cryptocurrencies for Investigators

By

Nick Furneaux – CSITech Ltd

Course Description

Cryptocurrencies in their many forms, based on the blockchain concept, are here to stay and will increasingly pervade the way people trade and create contracts with each other. This already provides a significant challenge for investigators from many different fields who are increasingly being faced with transactions that appear anonymous and incomprehensible.

This course, developed by respected investigator and researcher, Nick Furneaux, is designed to take an investigator from a basic understanding of blockchain technologies through to being an expert in the field, able to confidently investigate transactions and give evidence on their findings.

During the course, we build and then trade a simple new cryptocurrency in the classroom (NickCoin!) to understand all the basic concepts, even mining for new 'coins'. We learn about the underlying encryption and hashing algorithms used and what it teaches us about a transaction before setting up Wallets and trading on a primary blockchain.

Next, we learn how to find and extract addresses from paper wallets, computer disks/memory and the web. Then we look at how to extract raw data from all the primary blockchains using their API's and discover numerous techniques to de-anonymize users within the blockchain and even how to extract attributable Bitcoin addresses from a wiretap or seized device. Lastly, we consider how to seize and protect Coins used in criminal activity.

We are not aware of any course currently available that digs this deep into the subject. Although we cover Bitcoin and Ethereum specifically, the skills taught should enable the investigator to figure out the process of examining any cryptocurrency.

Course Goals

1. To learn and fully understand the blockchain concept
2. To be able to set up and run cryptocurrency accounts
3. To be able to locate addresses on various media including carving from memory
4. To be able to build information about a specific address
5. For the student to be able to track transactions
6. To enable the student to apply techniques to identify real world users in a transaction
7. To understand the methodology for seizure of Coins
8. To be able to explain the technology and your actions taken during the investigation

Course Content

Why do investigators need to understand Cryptocurrencies?

What is a cryptocurrency?

A look at many of the current lead currencies in the field

A detailed description of hashing as it applies to Cryptocurrencies, including the use of:

SHA256
Base58

A detailed understanding of blockchain cryptography including:

Public/Private Key encryption
RSA cryptography
Elliptic Curve cryptography

Build, run and trade a pseudo-cryptocurrency (NickCoin!) in the classroom which will teach the basics of the distributed ledger, transactions, hashing and mining

Comprehensive understanding of the blockchain including:

Block structure
Block headers
Deconstructing blocks from raw hex

- Hashing and the Merkle Tree
- Forks – Hard and Soft
- Interpreting raw data from Bitcoin and Ethereum

- Transactions
    - Pulling raw data via API's
    - Breaking down a raw transaction
    - How Change works
    - How fees work
    - What is the Mempool

- Mining – how it works
    - The Proof-Of-Work concept
    - The math's behind it all
    - Pools

- Wallets
    - Non-Deterministic
    - Deterministic
    - Hierarchical Deterministic Wallets (HD)
    - Hardware
    - Mobile Devices
    - Paper

- Setting up a covert wallet – how does the criminal do it?

Scripting - Understanding:

- Bitcoin scripts
- Ethereum Contracts
- Tokens
- ICO's

Setting up a wallet

- Full node

Investigations

Detecting the use of cryptocurrency

- Premises search, what to look for
    - Paper based material
    - Hardware wallets
    - QR and Mnemonic Codes

- Open Source Intelligence methods to locate addresses

Extracting information about a located address

- Using web based resources
- Using an API to get to the raw data
- Time analysis
- Searching for an address online

Extracting Private and Public keys (addresses) from seized computers

- Searching a computer for addresses
  - From an image
  - From RAM
  - Working on a live computer
  - Exporting Wallets
- Searching for wallets in backups

Opening and analyzing a recovered wallet

- Extracting all private and public keys
- Discovering what keys have been used
  - Batch address look ups
- Importing a 3rd party public key
- Cracking an encrypted Wallet

Following a transaction through the blockchain using online tools

- Following forked blocks
- Mixers

Following a transaction through the blockchain manually

- Using the Bitcoin Core console to interrogate the blockchain offline
- Using API calls to access any raw blockchain data online

Advanced Clustering

- Methods to identify addresses held by the same entity

Blockchain Visualization systems:

- Online tools –
  - Blockchain graph
  - Etherscan graph
- Maltego
- Numisight

Automatically Monitoring Addresses

IP address location and enumeration

IPs logged in the blockchain
Crawling for IP addresses in full nodes
Are they using Tor?
Mapping nodes against Tor IP’s

Tracking to a Service Provider

Currency exchanges
Traders
Thin client server admins

Using Open Source Methods
Investigating on the open web
Getting on the dark web

Extracting Address and Transaction data via an Intercept

Via Wifi monitoring
Via Wired Intercept

Detecting and decoding hidden micromessages

Methodology for seizing Coins using extracted Private Keys

Examples of crime

Money laundering

Illegal purchases

Phishing

For private keys
For donations

Hacking
Change addresses on web site

ICO fraud

Scripting and possible vulnerabilities

In depth, hands-on practical’s throughout the week.

Requirements

The student should have a reasonable understanding of investigation of online crimes, be computer literate and be comfortable with online researching. A basic understanding of cryptography, databases and fraud may be useful.