Crypto Fundamentals

JOHN BRIDGE
PRESIDENT, GOVERNMENT SECURITY
TRUST STAMP
JBRIDGE@TRUSTSTAMP.AI
706-751-5590

What do these companies have in common?

These are all peer-to-peer systems

- Facebook is among the world's largest media outlets but creates no content
- Alibaba, the world's largest shopping portal has no inventory
- Airbnb, the world's largest accommodation provider owns no real estate.
- Uber, the world's largest taxi company owns no vehicles
- Bitcoin, and blockchain create P2P for finance, contracts, etc. Decentralized Finance – financial transactions without banks.

Goals for Today

- Provide fundamental understanding of Blockchain/DLT
- Provide basic investigative techniques

bitcoin

What is Bitcoin?

- Designed as a peer-to-peer (P2P) value transmission system based on cryptography - a currency
  - Eliminates the need for a centralized third party (Federal Reserve, financial institution)
  - Not good or evil, just another 'format' for value transfer
  - Pseudonymous vs anonymous
- Can be used in true P2P or through online wallet service (Coinbase, eToro, BitFlyer, Kraken, etc.)
- No one owns (true p2p), transaction fees with exchanges.
  - Fees may be required by network.
- Push system, irreversible
- Many types of crypto-currencies, but bitcoin is the "gold standard"
- BTC created by "Satoshi Nakamoto"

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

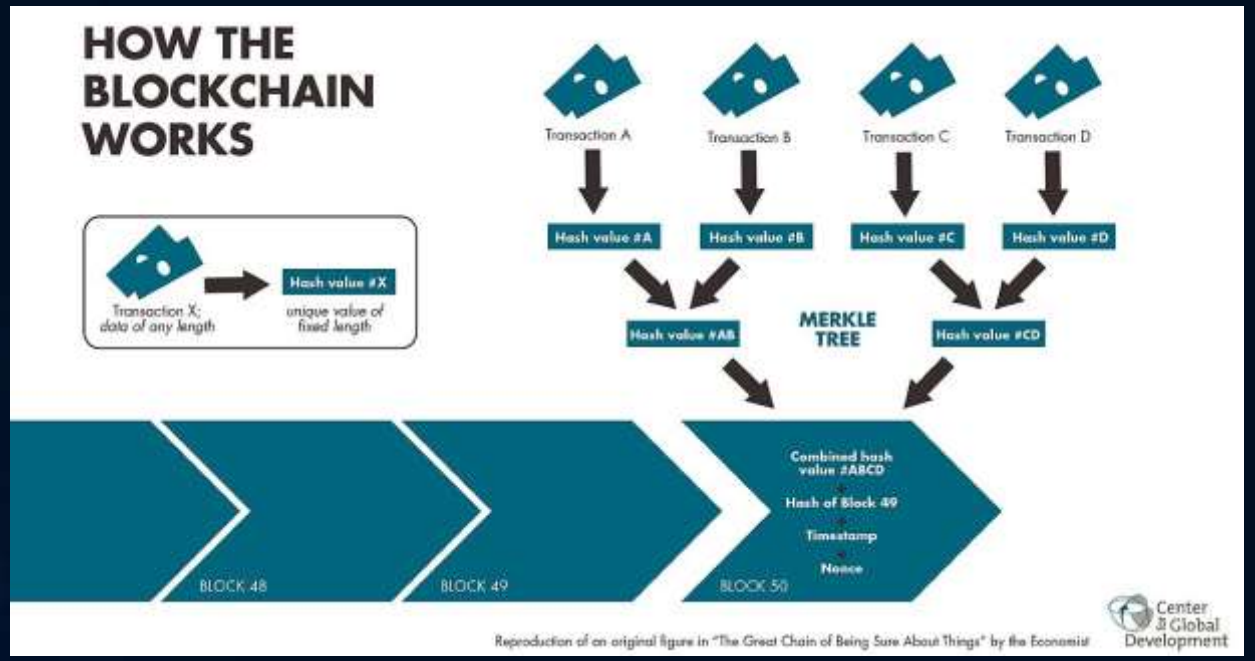
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Is the idea of a value transmission system that foreign to us?

What is Blockchain?

- A type of distributed ledger consisting of blocks of data. Each block is connected to the next block using a cryptographic hash referencing the previous block.



Wallets

- Wallets store btc public/private keys – electronic file
  - P2P versus online wallets
- Wallet addresses appear as hash values- string of numbers and letters
  - Ex. 1Q2cAA8EcdGpMZgFAwSpyCJVzqkTLsxNjs
  - Public key (wallet address) & private key
- Physical coin representations
- Quick reference (QR) codes
- Hardware wallets

The Blockchain

- Bitcoin's permanent public ledger
  - Record of all BTC transactions from current through beginning of BTC (2009)
    - Record shows wallet addresses used, amount, date, time
    - Connecting suspect to BTC wallet is up to the investigator
- Updated as BTC miners validate transactions and reach consensus
- When validated, new coins are generated in a "genesis" block.
- Much of bitcoin activity can be viewed on: https://blockchain.com/ with access to full blockchain by downloading open-source software at: https://bitcoin.org/en/download (miners)

What Does It Look Like?

- Wallets are hash values that appear as a series of numbers and letters. There are variations like physical coins and QR codes that represent those hash values.
- Wallet Example: bc1qr3kj9aflcwkylto6f82vpm5lthm82ajm376zxy
- How it appears on public ledger: https://www.blockchain.com/btc/address/bc1qr3kj9aflcwkylto6f82vpm5lthm82ajm376zxy
- Bitcoin "Stock Tickers"
  - http://www.coindesk.com/
  - https://coinmarketcap.com/

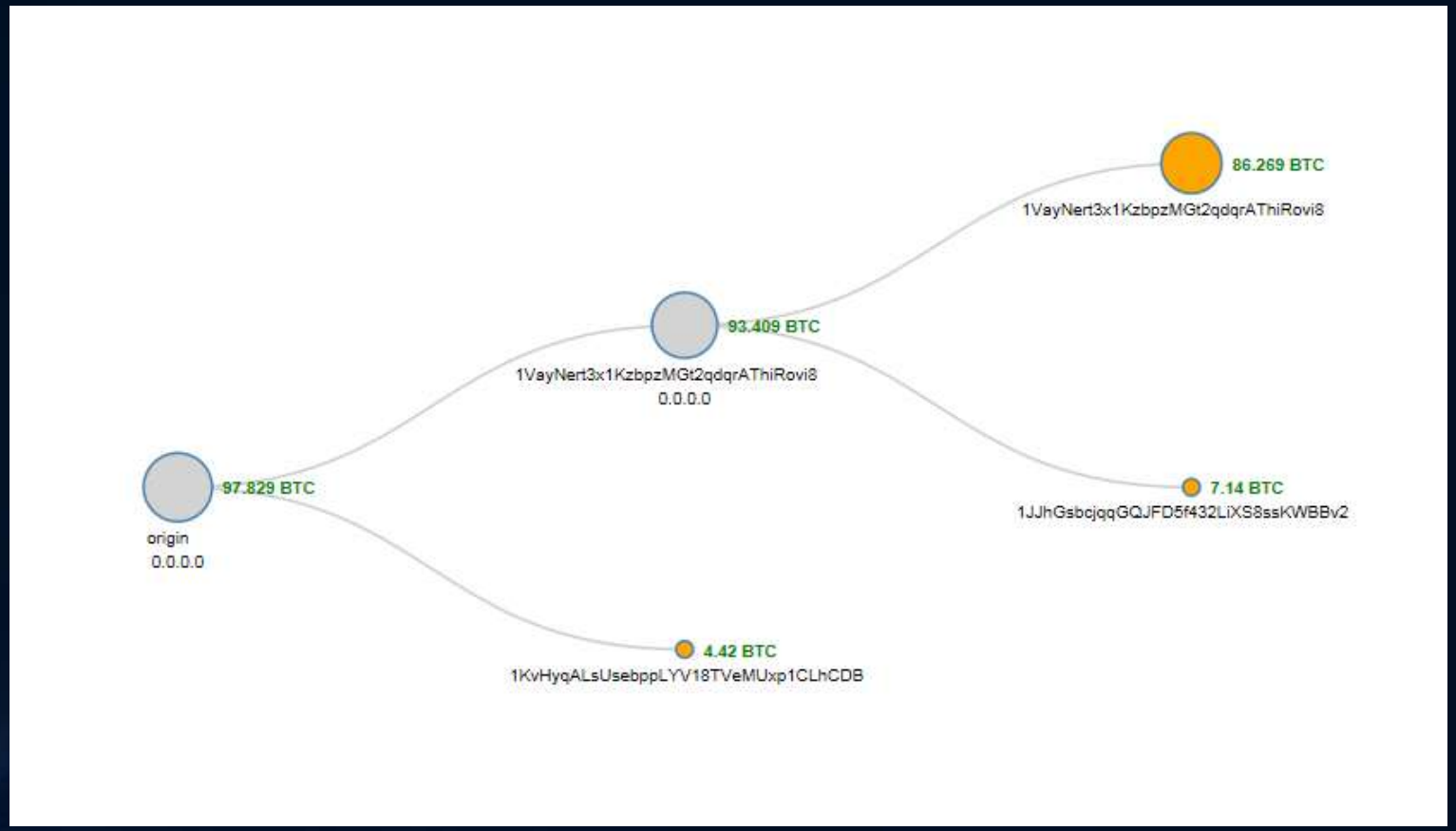
Example of a Bitcoin Wallet

Bitcoin address 1MpmhCc9yq5Sj78f83zLdvUQFK3E4s9xpz

Hash	e46b5fb1b1162e1e04bebba241d71821a433acff
Number of confirmed transactions	4
First transaction	753 days ago
Last transaction	411 days ago
Total Received	25.8 mBTC
Balance	0 BTC

Transaction 28d8cf3389c7b7b7da29091f294e3c07b42fbceca00aff48bd9f444e54519d49 (fees: 8.22 mBTC)

Blockchain Visualize Tool



What's the Big Deal?

- BTC, in current form, can be more efficient than current financial solutions because the centralized 3rd party is eliminated
- Blockchain can create trust between two parties (or more) who do not know each other.
- Blockchain works well for financial transactions, but potentially for any situation in which the need for a 3rd party is not ideal (smart contracts).
  - Legal documents/agreements, voting, authentication, doc storage, supply chain
- Can work well for merchants without volatility risk
  - Instant currency conversion, no chargebacks
  - Increasing number of merchants like Overstock, Home Depot, Starbucks and AirBnB.

Mining & Validation

- Bitcoin 'Miners' operate computers and BTC software that are part of the transaction validation process
- P2P BTC transaction initiated (Ex. John sends Doug one bitcoin)
  1. Cryptographic problem transmitted to miners (billions hash computations/sec)
  2. Once 1st miner solves the problem (proof of work), trans to other miners (date/time) to verify
  3. Transaction is validated by consensus (while eliminating the need for third party validation). Permanent & Irreversible . Transaction visible in near real-time. Blocks resolve roughly every ten minutes..
  4. Transactions fully validated within approximately two hours.

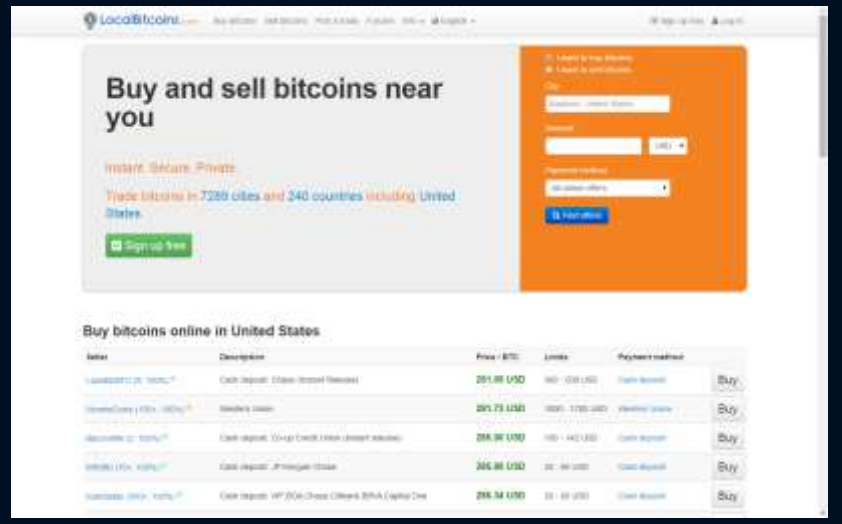
Mining & Validation

- 'Winning' miner is rewarded with newly created BTC – the mining function
  - 21 million BTC limit and created at pre-determined rate (halved every 210,000 blocks)
    - Cryptographic problems get more difficult as BTC is mined
    - Inflationary control
- Currently, between 160-180 million terahashes (trillion) computations/sec in computational power mining BTC (160-180 quintillion per second worldwide)
- Bitcoin mining consumes one-half percent of worldwide energy. The network consumes the equivalent of the amount of power generated by 8-9 nuclear plants.

Bitcoin Mining Rigs

How is BTC initially obtained?

- In person transactions (https://localbitcoins.com)
  - App-based payments
  - Physical representations (coins, hardware wallets, etc)
- Exchanges (Coinbase, eToro) - registered MSBs
- Buying/Selling a product for Bitcoin
- Mining (participating in the validation process)
- Cypto Currency ATMs (CoinCloud, CoinStar):
  - locations (http://coinatmradar.com/)
- Online "Faucets" (eg freebitco.in). Beware scams.



Coinatmradar.com screenshot

Bitcoin ATMs

Bitcoin Faucets

- Websites like 99 bitcoins
- Can "get your feet wet"
- Free bitcoin in very small amounts.
- Requires email address and validation.
- Creates an account related to a wallet.
- Opportunity to experiment with someone else's money.
- Requires actions like watching ads.

Non-Fungible Tokens (NFTs)

- NFTs are tokens that we can use to represent ownership of unique items. They let us tokenize things like art, collectibles, even real estate. They can only have one official owner at a time and they're secured by the Ethereum blockchain – no one can modify the record of ownership or copy/paste a new NFT into existence. (Ethereum protocol) Fractals are a new concept on BTC chain.
  - There are other protocols that NFTs can be traded on as well (Stellar, Neo…)
  - Example taken from Foundation.app
    - Price is 1 ETH (over $4,000)

Decentralized Finance (DeFi)

Decentralized finance, also known as DeFi, uses cryptocurrency and blockchain technology to manage financial transactions. DeFi aims to democratize finance by replacing legacy, centralized institutions with peer-to-peer relationships that can provide a full spectrum of financial services, from everyday banking, loans and mortgages, to complicated contractual relationships and asset trading. (Forbes)

- Uniswap (Decentralized Exchange)
- MakerDAO (Lending Protocol)
- Aave (Lending Protocol)

∞dlesBlockchain

	Traditional	Fintech	DeFi
Issuing money	The State	-	Proof of Work and Proof of Stake rewards
Transferring money	Cash	Revolt, Transferwise	Cryptocurrency and token transaction
Lending/borrowing Money	Banks	Lending Club	Tokenized P2P debut
Exchange assets	Exchange & Brokers, like Nasdaq	-	Decentralized exchange
Investing money	Stocks, Bonds, etc, accessible though banks and exchange	Robinhood	Tokenized financial products (ICOs, STOs and Token baskets)

blockchain.oodles.io

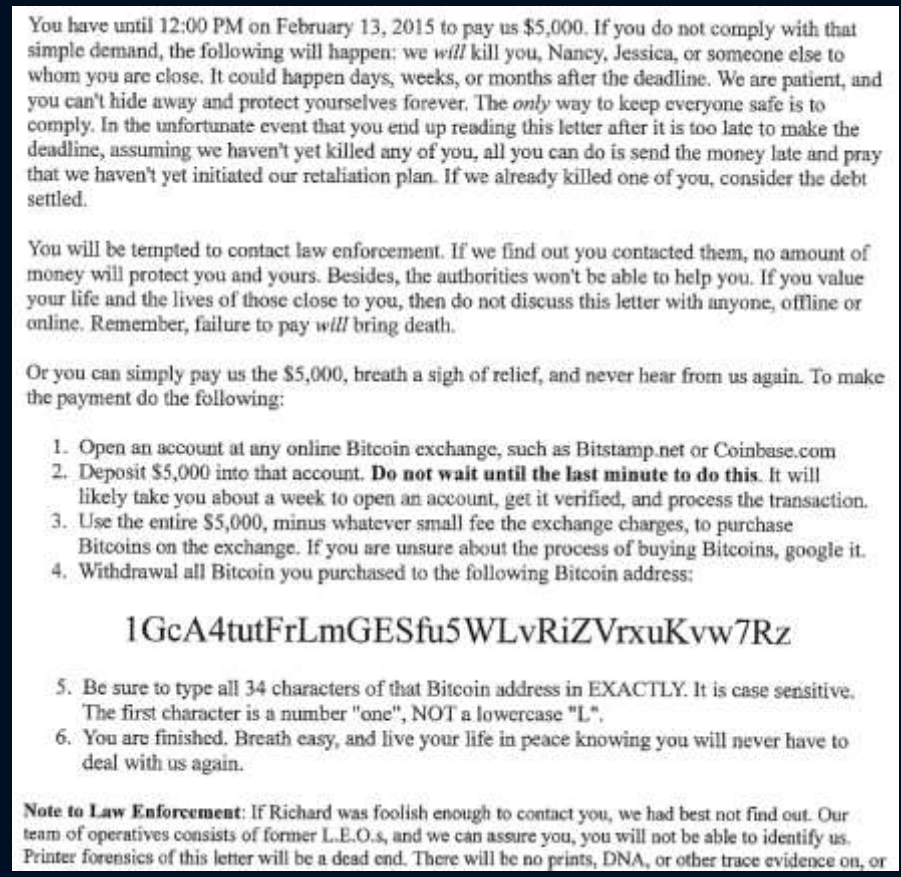
AML Considerations

- Dark Net / Dark Market
  - Accessible only through TOR (The Onion Router) which anonymizes users web activity by utilizing multiple proxy servers
    - Bounces from many different servers in different countries

- BTC has been popular in the dark market where many illegal items are sold including compromised credit card data
  - Push system, irreversible, instant, no chargebacks (unlike credit cards)
  - Crypto currencies can be pushed through tumblers that co-mingle currency making it more difficult to track through the blockchain
  - In the U.S., online currency exchanges like Coinbase and Bitstamp are required to register as MSBs and follow AML rules
  - FATF Travel Rule was supposed to apply to all VASPs as of 2020.

Bitcoin-Based Scams

- This is an actual letter.
- Information gleaned from public sources and social media used to exploit victim.
- Requests funds to be sent to a bitcoin address.
- Even had the audacity to threaten any law enforcement who might become involved.



You have until 12:00 PM on February 13, 2015 to pay us $5,000. If you do not comply with that simple demand, the following will happen: we *will* kill you, Nancy, Jessica, or someone else to whom you are close. It could happen days, weeks, or months after the deadline. We are patient, and you can't hide away and protect yourselves forever. The *only* way to keep everyone safe is to comply. In the unfortunate event that you end up reading this letter after it is too late to make the deadline, assuming we haven't yet killed any of you, all you can do is send the money late and pray that we haven't yet initiated our retaliation plan. If we already killed one of you, consider the debt settled.

You will be tempted to contact law enforcement. If we find out you contacted them, no amount of money will protect you and yours. Besides, the authorities won't be able to help you. If you value your life and the lives of those close to you, then do not discuss this letter with anyone, offline or online. Remember, failure to pay *will* bring death.

Or you can simply pay us the $5,000, breath a sigh of relief, and never hear from us again. To make the payment do the following:

1. Open an account at any online Bitcoin exchange, such as Bitstamp.net or Coinbase.com
2. Deposit $5,000 into that account. **Do not wait until the last minute to do this**. It will likely take you about a week to open an account, get it verified, and process the transaction.
3. Use the entire $5,000, minus whatever small fee the exchange charges, to purchase Bitcoins on the exchange. If you are unsure about the process of buying Bitcoins, google it.
4. Withdrawal all Bitcoin you purchased to the following Bitcoin address:

1GcA4tutFrLmGESfu5WLvRiZVrxuKvw7Rz

5. Be sure to type all 34 characters of that Bitcoin address in EXACTLY. It is case sensitive. The first character is a number "one", NOT a lowercase "L".
6. You are finished. Breath easy, and live your life in peace knowing you will never have to deal with us again.

Note to Law Enforcement: If Richard was foolish enough to contact you, we had best not find out. Our team of operatives consists of former L.E.O.s, and we can assure you, you will not be able to identify us. Printer forensics of this letter will be a dead end. There will be no prints, DNA, or other trace evidence on, or

Investigative Vectors

- Shipping – if someone is selling illegal goods, how are they shipping?
  - Possible shipping accounts so drop locations can be used - Suspect info
  - Shipping is a common investigative vector for illegal online stores
- Tracking movement of funds in the blockchain (Ciphertrace, BIG, Chainalysis)
- Funds moving through an online wallet service (MSB) are likely to have records
  - Associated checking account – debit/credit entries from btc wallet services?
  - Multiple accts/transactions crossing the same MSB platform.
  - Subpoenas
- Bitcoin ATMs may have cameras

Dark Web Considerations

- Are they leaking their real IP address through other programs? (Apple iTunes, anti-virus program)
- Tracking Cookies
- Dark Web honeypots (direct linking with potential targets to "unmask" them).
- If you are conducting investigations in the dark web, consider OpSec on your own presence. Malware is also abundant…use a dedicated computer.
- FinCen recently released report that many IPs reported on Filing reports were from TOR. Banks should indicate TOR IPs on the Filings and consider blocking TOR IP addresses.
- Dark web investigations should be done by someone with expertise.

NC Case Study

- Warrants were issued in Raleigh, NC for suspect on Drug Charges.
- Suspect was using the Darkweb to facilitate his drug trade.
- The currency of choice in the dark web is Bitcoin. Bitcoin is difficult to trace and believed to be “anonymous.”

Case Study

- Suspect had a known account at a NC based bank. He was using an LLC as well as a personal acct.
- This bank revealed transactions to both Coinbase and CoinRnr.
- These are both MSBs for Bitcoin transactions.

Case Study

- Information obtained from the MSBs indicated that Suspect's activity was consistent with money laundering, so they shut his account down and filed.
- There were five other banks associated with the Digital Currency MSBs.
- One MSB shut suspect out of his account but indicated there was a small BTC balance in his acct.
- That MSB sent suspect an email indicating his account would be unlocked for 30 days for him to remove the BTC in his account.

Case Study

- IP address was captured when he returned to the MSB internet platform.
- That IP address was a proxy address that resolved to The Puffin Browser.
- The IP is hosted by Hurricane Electric in California.
- Contact was made with Hurricane to use the known information to track back to the originating IP address. Suspect was captured before this court order was returned with the information.

Case Study

- Investigation continued with the other accts captured by the MSBs.
- One financial institution noted transactions with FedEx.
- FedEx noted more than 70 transactions recently. Nothing was current.
- People selling drugs in the darkweb need to ship!

Case Study

- An internet-based bank identified by the MSB showed transactions in Guatemala.
- Marriott ATM transaction revealed no Marriott in Guatemala. Outdated info on ATM.
- The last transaction was at a bus station in Guatemala.

Case Study

- Another bank identified by the MSB picked up transactions after the internet bank transactions ceased.
- This bank indicated a car rental from Hertz in San Pedro Sula.
- There were also transactions in Puerto Cortez, a beach community on the coast.

Case Study

- State Dept and local immigration went to Hertz and had them call Crawford to advise his car needed service and offer an upgrade.
- Suspect was arrested at the Hertz rental location and was deported two days later for illegal entry.

New York Case

- Suspect hired Mark Zuckerburg to create a website before he created Facebook.
- Suspect forged documents to make it appear that he commissioned the creation of Facebook. Sued for significant ownership stake.
- Court charged him with forging documents and placed him on electronic monitoring.
- Removed ankle monitor and rigged to ceiling fan with timer to simulate movement to buy time to flee.

Case Study

- FinCen research led to transaction through Circle
- Circle supporting documents led to a prepaid card with an Irish Bank. Bank pointed to potential locations in Portugal and/or Spain.
- Account was blocked, Irish bank did not have additional information, but led to parallel investigation of possible crypto transactions.
- Sent suspect cryptocurrency through a CI, but the money remained in the wallet (that had never previously been used).
- Checked wire remitters for transactions. Found transactions to Peru and Ecuador.

Case Study

- Transactions to Ecuador included a name, address and contact information.
- Working with Ecuadorian authorities, suspect was arrested at a banana plantation.
- Suspect successfully fought extradition and remains in Ecuador.

QUESTIONS?