

Busting the Blockchain: How To Trace & Seize Virtual Assets & Evaluate Risk in a Pseudo- Anonymous World

Josias N. Dewey, Partner, Holland & Knight LLP
London, U.K.

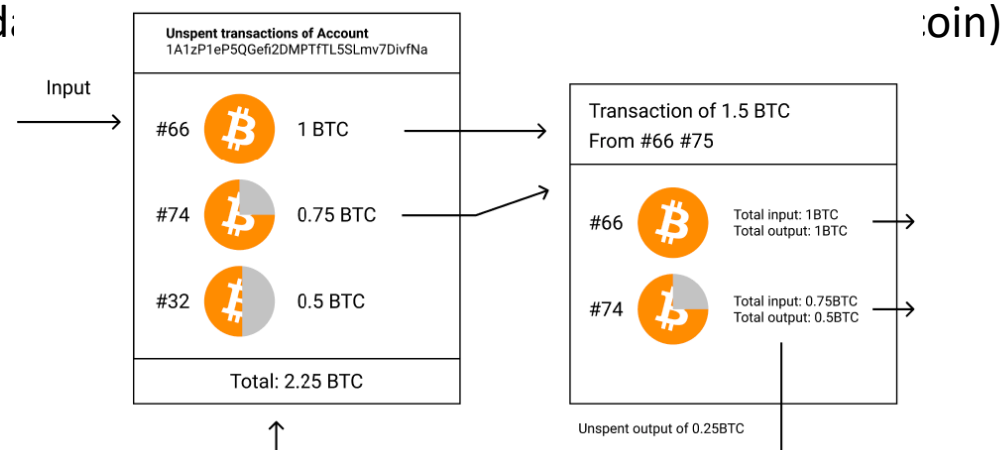
November 12, 2019

Introduction

Types of Virtual Assets

Transparent

- Bitcoin and its direct and indirect descendants:
 - Unspent transaction outputs (UTXO)
 - Pseudo-anonymous
 - Rules established by protocol
 - Highly liquid
- Ether and Ether Classic
 - Accounts based
 - Pseudo-anonymous
 - Rules established by protocol
 - Highly liquid
- ERC tokens (e.g., ERC-20 tokens, ERC-721 tokens)
 - Same as Ether
 - Can store in any wallet that can hold ether but may not be able to transact with it.
 - Rules arise out of token contract that created
 - Liquidity varies from high to illiquid
- Other native virtual currencies (e.g., XRP, Lumens)
 - Pseudo-anonymous

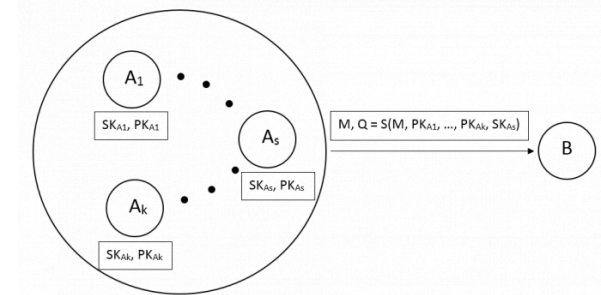
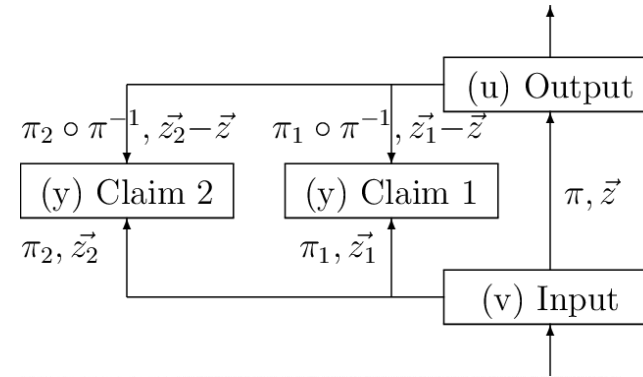


From:	0xa0543f6a3af5f7ae34c6432884067f6cfc042e81
To:	0x3147a6ba4b5b017b4a10554a17b5be01954f2d7b
Value:	0.0006 Ether (\$0.11)
Transaction Fee:	0.00042 Ether (\$0.08)

Types of Virtual Assets

Opaque

- ZCash
 - Zero-knowledge proofs
 - Can be masked or unmasked
 - Two types of addresses: Shielded and Transparent
 - Shielded is untraceable
- Monero
 - Ring-signatures
 - Untraceable
- DASH
 - PrivateSend
 - Master nodes



Coinbase drops UK support for privacy-focused Zcash cryptocurrency

ZEC deposits will be automatically converted to British pounds if they are not moved elsewhere.

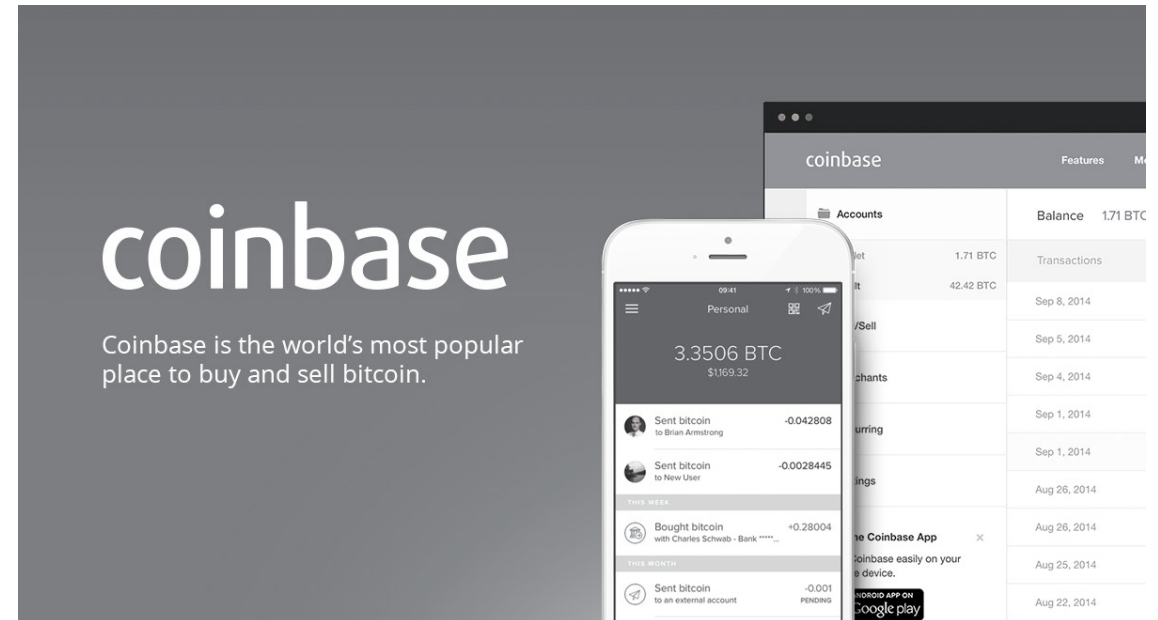


By [Charlie Osborne](#) for [Between the Lines](#) | August 13, 2019 -- 11:17 GMT (04:17 PDT) | Topic: [Blockchain](#)

How do you hold?

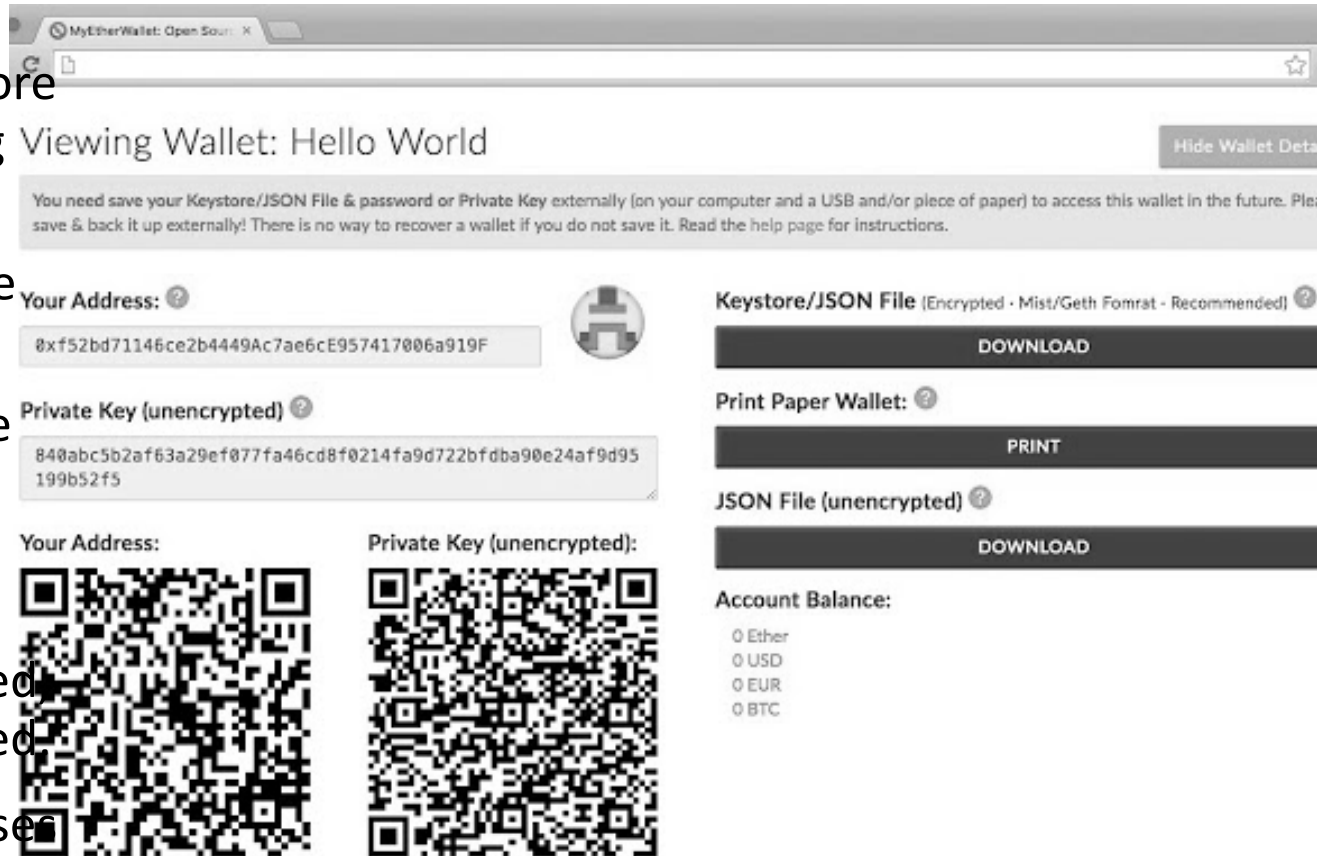
Hosted Wallets:

- Hosted wallets are wallets hosted by third party, which third party controls the private keys.
- The benefit is that user doesn't need to worry about managing keys.
- The risk is that the third party handles keys properly.
- Don't send account statements.
- Don't issue 1099s.



Software Wallets:

- Software wallets are software based wallets that typically store private keys on device running the software.
- The user generally controls the private keys.
- If loses private key or is unable to decrypt it, the virtual currency is lost.
- If computer running the software wallet is compromised, private keys may be intercepted.
- Connecting to network increases security vectors.



The screenshot shows the MyEtherWallet interface in a browser window. The title bar reads "MyEtherWallet: Open Sour...". The main heading is "Viewing Wallet: Hello World" with a "Hide Wallet Deta" button. A warning message states: "You need save your Keystore/JSON File & password or Private Key externally (on your computer and a USB and/or piece of paper) to access this wallet in the future. Please save & back it up externally! There is no way to recover a wallet if you do not save it. Read the help page for instructions." Below this, the "Your Address:" is displayed as "8xf52bd71146ce2b4449Ac7ae6cE957417806a919F" with a QR code to the right. The "Private Key (unencrypted)" is shown as "840abc5b2af63a29ef077fa46cd8f0214fa9d722bdfdba90e24af9d95199b52f5" with a QR code to the right. On the right side, there are three sections: "Keystore/JSON File (Encrypted - Mist/Geth Fomrat - Recommended)" with a "DOWNLOAD" button; "Print Paper Wallet:" with a "PRINT" button; and "JSON File (unencrypted)" with a "DOWNLOAD" button. At the bottom right, the "Account Balance:" is shown with radio buttons for "Ether", "USD", "EUR", and "BTC".

Hardware Wallets:

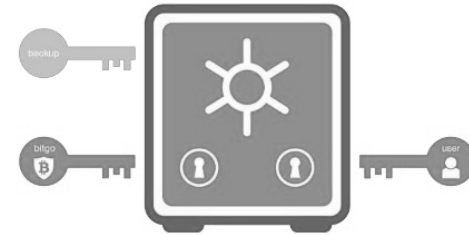
- Hardware wallets are physical devices that store private keys and have embedded software capable of building and signing transactions.
- The user generally controls the private keys.
- If loses private key (and backup words) or is unable to decrypt it, the virtual currency is lost.
- Most hardware wallets will not expose private keys to computer when connected for purposes of broadcasting transactions.
- Risk of device being physically damaged.



Multi-Sig Wallets and Other Safeguards

- Need more than one private key to sign transaction.
- Can set-up several variations, 2 of 3, 3 of 5 and so on.
- Consider for custodial relationships.
- Be careful of biometric safeguards.
- No guarantee that retinal scan or fingerprint scan will be possible after decedent passes away (e.g., plane crash)

Multi-Sig: The Digital Equivalent of a Safe Deposit Box



Multi-sig! ☺ 335Zc8furTKgD32bWewYwGYGai7sMrtKse

Not multi-sig ☹ 19frDKN7XwWL2wwhz35as7PtrFcL4vCNYG

BitGo™

10

Copyright © 2014 BitGo, Inc.



Tuur Demeester
@TuurDemeester



Critical Parity bug leaves +\$150M in \$ETH frozen, including \$90M of Gavin Woods' Polkadot ICO. Cue clamoring for new hard-fork bailout... [twitter.com/petertoddbtc/s...](https://twitter.com/petertoddbtc/status/911111111)

2:30 PM - Nov 7, 2017

🗨 37 ↻ 242 ❤ 363



Patrick McCorry
@paddyucl



Over 1 million ether (around \$278,359,059 US) is the total impact of @ParityTech based on pastebin.com/ejakDR1f [docs.google.com/spreadsheets/d...](https://docs.google.com/spreadsheets/d/...)

1:08 PM - Nov 7, 2017

A screenshot of a spreadsheet with columns for 'Contract', 'Balance', and 'Ether'. The data shows a large sum of ether.

Parity Hack in numbers

Sheet1 Contract, Balance\$\$, Ether
0x376c3e5547c68bc26240d8dcc6729fff665a4448
34, 459, 861. 59, 114, 939
docs.google.com

🗨 7 ↻ 95 ❤ 119



How easy is it to create crypto?

HKKOIN

HKKOIN entitles you to absolutely nothing! But you could win an iPad!

- public address: `0xb7B46AAD111A77343bB8672d0fF9b22bB45336dD`



- private key:
`0x5732e54786dba530360f532634efd141c477a41e9d3836f183ef73d64035d67a`



Recovering Assets



Unique Concerns

- Virtual currency can exist in any form capable of storing alpha-numeric strings—including the human brain.
- Just because you have a copy of the private key doesn't mean someone else doesn't have another copy.
- Avoid protocols allowing individuals access to private keys without multi-sig or other measures in place.
- Consider proper procedures that should be in place with any cyber consultants and/or law enforcement.
- Log all access to materials containing private keys.
- Avoid e-discovery vendors.
- Immediately transfer all tokens to new addresses controlled only by receiver.
- Safely store private keys and recovery seeds in multiple locations. Entrust only half recovery words with different individuals.
- AVOID BIOMETRIC security systems.
- Hosted wallet vs. hardware wallet.
- Insurance?

Proper Protocols

- Agents who investigated Silk Road drug marketplace ultimately arrested for stealing BTC seized during take down.
- Be sensitive in communicating information or documents that contain private keys or passphrases.
- Pay particular care to redact private keys from email and other written communications that may be turned over.
- If can't (e.g., grand jury subpoena), then make sure to alert the receiving party about the sensitive nature of the communications.

Private key

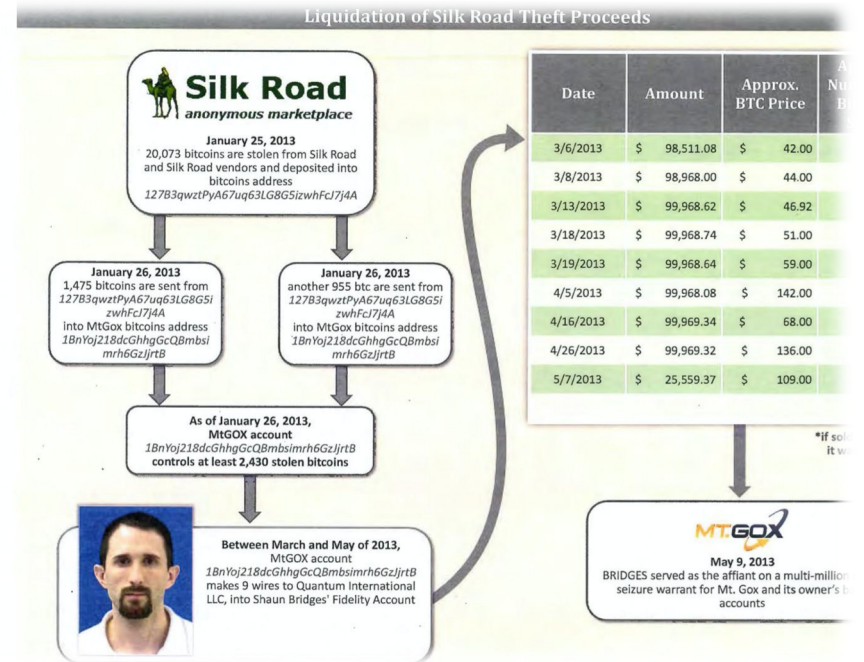
5Hwgr3u458GLafKBgxtssHSPqJnYoGrSz

Bitcoin address (normal)

17VZNX1SN5NtKa8UQFwxQbFeFc3iqRY

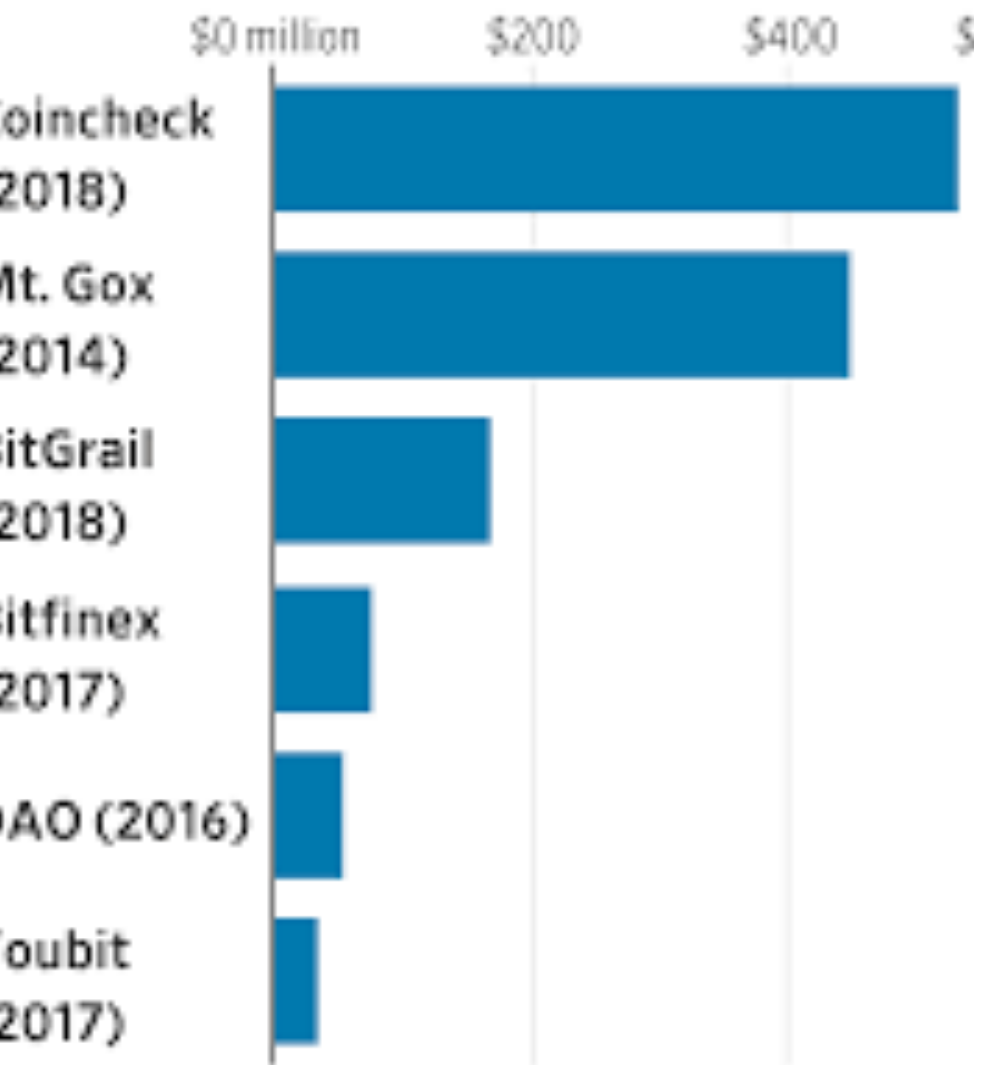
Bitcoin address (multisignature)

3EktnHQD7RiAE6uzMj2ZiFT9YgRrkSgzQ



Black Attack

Select losses from cyberattacks on
cryptocurrency trading, investing platforms



Source: The companies

Best Practices

- Log all access to materials containing private keys.
- Avoid e-discovery vendors and other third-party access.
- Immediately transfer all tokens to new addresses controlled only by receiver.
- Safely store recovery words in multiple locations. Consider storing only half of recovery words with different individuals.
- AVOID BIOMETRIC security systems.
- Is it better to hold in hosted wallet (e.g., Coinbase) or hardware wallet? Pros and cons?
- Protection through insurance?

Unsettled Questions as to Nature of Asset

- A fundamental question remains unanswered about how to treat virtual currency and tokens.
- Should it be treated like cash? It seems to trade hands like cash, but unlike cash, most virtual currency is easily traced back to its owner because of the blockchain's transparency.
- Or should it be treated like other personal property? If someone steals your TV, and it's later recovered from unsuspecting person who purchased it, the TV is returned to original owner. Does this apply to virtual currency?
- Fairly important question given over \$1 billion in virtual currency has been stolen during the last 18 months.
- If we treat like ordinary, traceable property, there will be a chilling effect on its use in commerce.
- Even more complicated if inconsistent cross-border treatment.
- A person can cross borders with access to \$1 billion with nothing but the alphanumeric string he or she has memorized.



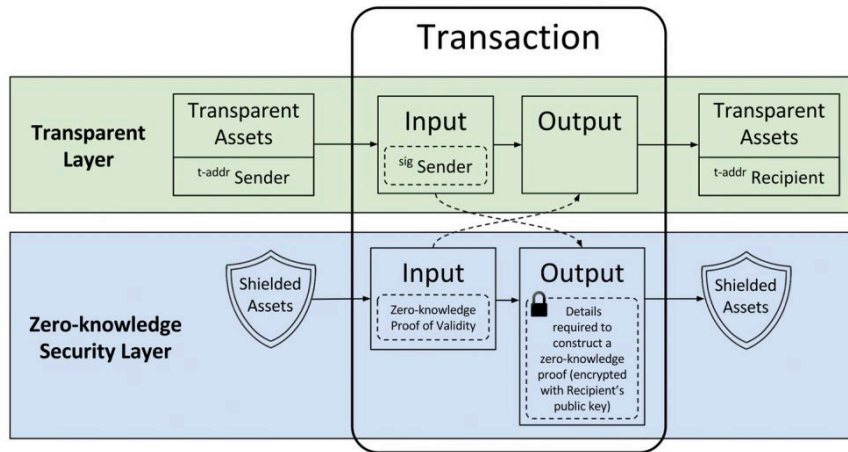
Preserving Assets

- Determining when to sell virtual assets.
 - ❖ Immediately?
 - ❖ Wait and see?
 - ❖ Evaluate market conditions?
- Can a receiver or other custodian sell all the virtual currency?
 - ❖ Company's native token
 - ❖ BTC and ETH etc. raised during the sale
 - ❖ Other tokens acquired by company from proceeds of the sale
- Distribution agents and similar providers may be asked to return virtual currency rather than cash from liquidation. Consider ways to leverage smart contracts to reduce overall cost of administration.



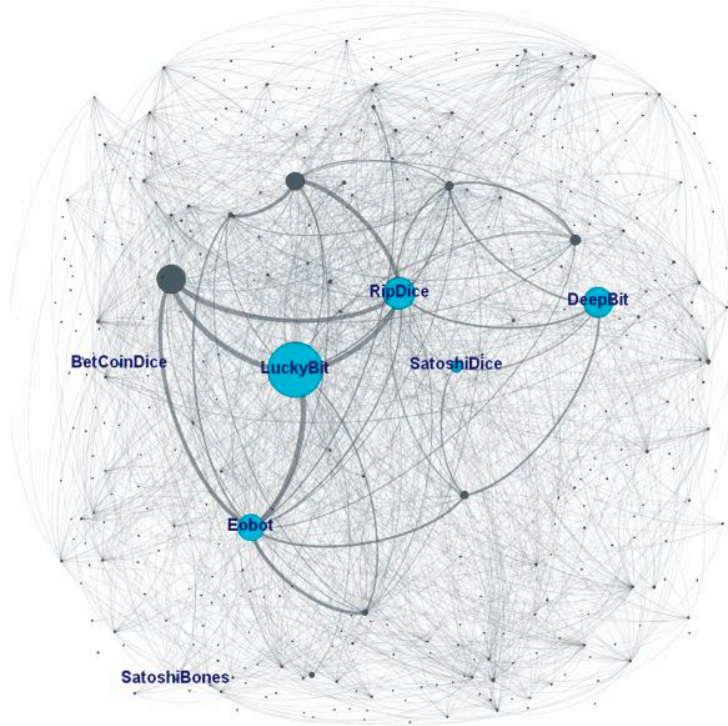
Data security and virtual currency

Anatomy of a Crypto Theft (Post-Breach)



- Over \$1 billion in virtual currency stolen over last 24 months.
- Cat and mouse game between law enforcement and criminals.
- Criminals need way to move virtual currency into fiat currency outside regulated exchange.
- BTC-e was preferred laundering partner until it was taken down in the summer 2017.
- Many criminals turned to Shapeshift, which allowed anonymous users to exchange one type of virtual currency for another.
- For example, ETH and BTC could be exchanged for Monero and Z-Cash—neither of which can be effectively traced or followed on a blockchain.
- Late 2018, Shapeshift succumbs to pressure and requires KYC.
- Next weak point?

There is hope



- With the exception of virtual currencies like Monero and Zcash, most blockchains are very transparent.
- Powerful data analytics tools can level the playing field.
- We hired MIT PhD to build a solution that leveraged network graphing and structured databases to follow virtual currency across blockchains and identify touch points with regulated exchanges.
- Technique has been used to seize and identify the location of a significant amount of assets, as well as identify one or more individuals likely associated with hackers.
- Next weak point?
- Working on updates to platform to identify market manipulation activities.

Compliance and AML/KYC

BSA EXPECTATIONS ON VIRTUAL CURRENCY-RELATED BUSINESSES

“BSA requirements and supervisory expectations for providing banking services to administrators or exchangers of virtual currencies are the same as money transmitters.” See *FFIEC BSA/AML Examination Manual* at p. 303.

Key Terms

Virtual Currency: A medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction.

User: A person that obtains virtual currency to purchase goods or services.

Exchanger: A person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.

Administrator: A person engaged as a business in issuing (putting into circulation) a virtual currency,

BSA EXPECTATIONS ON VIRTUAL CURRENCY-RELATED BUSINESSES

Risk Assessment

The financial institution should perform an effective MSB Risk Assessment that, among other things, considers the following factors:

- Purpose of the account.
- Anticipated account activity (type and volume).
- Types of products and services offered by the MSB.
- Locations and markets served by the MSB.

Enhanced Due Diligence

- Understand sources of virtual currency.
- Must look beyond last transaction. If virtual currency associated with underground darknet marketplace two hops from customer, that could raise risk issues.
- Also, must evaluate outbound transfers of virtual currency.
- Identify transaction patterns associated with illicit or high risk activities.
- Need analytics tool to properly evaluate.

Conclusion

- Specialized assets and operating companies with unique business models may require specialized expertise and technology.
- First “24 hours” is often mission critical. Need ability to move quickly.
- Utilizing technology and thinking outside the box (e.g., using data analytics tools to foster asset recovery) becoming critically important.
- Can’t afford to rely exclusively on law enforcement.
- Focus on compliance and risk mitigation only becoming more important.