



# Cryptocurrency Scams and Frauds: A View from the Dark Side

---

## VIGILANCE

<https://vcci.io>

© 2024 Finrock Group LLC, All Rights Reserved

1



### Roadmap



- Cryptocurrency and Blockchain Primer for Fraud Investigators
- Investigative Techniques for Incidents Involving Cryptocurrency
- Common Cryptocurrency Scams and Frauds
- Pig Butchering Case Study
- Nation State as a Criminal Organization: North Korea

2



## Bitcoin and Blockchain Basics



3

3



## What is Cryptocurrency?

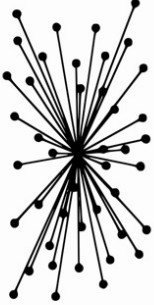
**Cryptocurrency:** A digital currency in which transactions are verified and records maintained by a decentralized system (blockchain) using cryptography, rather than a centralized authority.




4

4

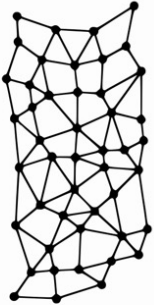
## What is a Blockchain



Centralized



Decentralized



Distributed

**General Ledger Sheet**

Account: <input style="width: 80%;" type="text"/>				Sheet No: <input style="width: 50%;" type="text"/>		
				Account No: <input style="width: 50%;" type="text"/>		
Date	Description	Journal ref.	Transaction		Balance	
			Debit	Credit	Debit	Credit
<b>Total</b>						

5

5

## Cryptocurrency Wallets

Location where cryptographic keys to access your cryptocurrency on the blockchain are stored; Wallets can be hot or cold.

Exchange based wallet

Desktop wallet

Mobile Wallet

Hardware Wallet

Paper Wallet










17A16QmavnUfCW11DAApiJxp7ARnxN5pGX

6

6



## Cryptocurrency Exchanges

**Exchange:** A marketplace where crypto is bought, sold, or exchanged for fiat or other crypto (PII holder)

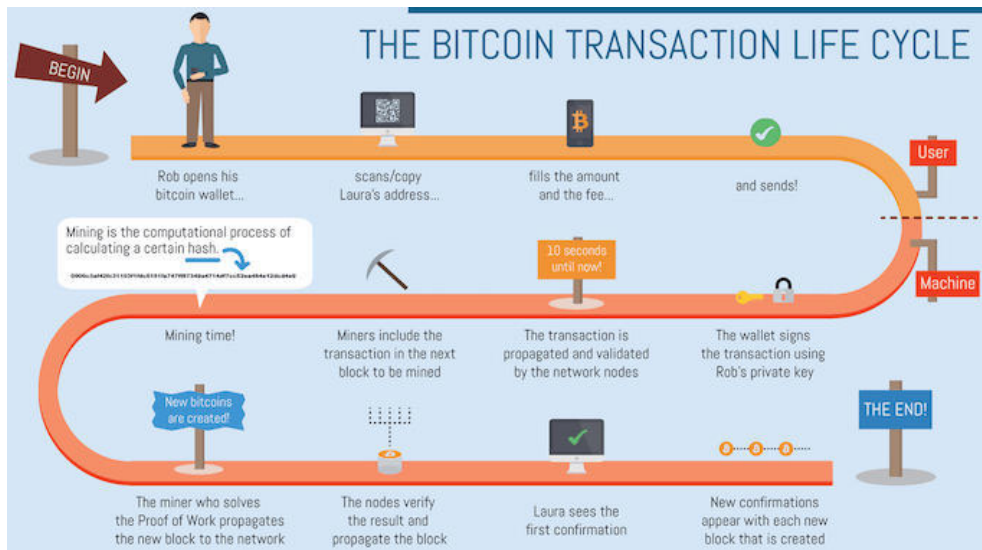


7

7



## How A Bitcoin Transaction Works



8

8



### What is Money?



Unit of Account

Store of Value

Medium of Exchange



### Cryptocurrency is Value Agnostic



Like a US Dollar, a car, a cell phone, the internet, and a gun

No independent value system

International Finance + Computer Science + Made Up Terms = Confusion



## Investigative Techniques



11

11



## Cryptocurrency is not Anonymous

**Anonymous vs Pseudonymous**

- Cell Phone Numbers
- Bank Account Numbers
- Social Security Numbers
- Mobile Ad Id



12

12



## Can We Still Track Movements of Funds?

### Follow the Money

Tracking cryptocurrency using blockchain analytics

Identifying wallet addresses

Analyzing money movement

Establish patterns and aggregation wallets (pass through accounts and concentration accounts)

Follow to fiat on/off ramp (exchange) where there is KYC/AML Information



## Investigative Techniques

blockchain.com/explorer/addresses/btc/bc1qw2aztud5yypwvatr45a4yqwdlvf4q4rxzidx

bc1qw2aztud5yypwvatr45a4yqwdlvf4q4rxzidx

Blockchain.com

Home Prices Charts NFTs DeFi Academy News Developers Wallet Exchange Bitcoin

Summary

This address has transacted 14 times on the Bitcoin blockchain. It has received a total of 1.90677024 BTC \$131,657 and has sent a total of 1.63425542 BTC \$112,841. The current value of this address is 0.27251482 BTC \$18,816.47.

Total Received	1.90677024 BTC	\$131,657
Total Sent	1.63425542 BTC	\$112,841
Total Volume	3.54102566 BTC	\$244,499
Transactions	14	

Transactions

ID: b41f-0b27	3/11/2024, 17:00:22	From bc1q-y6s8 To 35 Outputs	0.05692822 BTC • \$3,930.75 Fee 41.2K Sats • \$28.43
ID: 13d4-1011	3/02/2024, 17:14:49	From 9 Inputs To bc1q-xldx	0.00722644 BTC • \$498.97 Fee 26.7K Sats • \$18.42
ID: ada8-9cbd	1/31/2024, 14:34:10	From bc1q-xldx To 2 Outputs	-0.00044177 BTC • -\$30.50 Fee 4.2K Sats • \$2.88

## Investigative Techniques

https://addresses/BTC/bc1qtj39e75wajdlmu5ctp44zp3narg5gch3dxv9lv

bc1qwt2aztud5yypwvatr45a4yqwdlvf4q4rxzldx

<b>From</b> 1 bc1qtj39e75wajdlmu5ctp44zp3narg5gch3dxv9lv 0.00040000 BTC • \$27.68	<b>To</b> 1 bc1qtj39e75wajdlmu5ctp44zp3narg5gch3dxv9lv 0.00013384 BTC • \$9.26 2 bc1qte4eg9vg0ghpechrhe6ftc8lz5*7fvy90yk8za5 0.00021635 BTC • \$14.97
ID: 0247-ea88 3/27/2024, 11:27:33	
From bc1q-8za5 To 2 Outputs 0.00021631 BTC • \$14.97 Fee 5.1K Sats • \$3.56	
<b>From</b> 1 bc1qte4eg9vg0ghpechrhe6ftc8lz5*7fvy90yk8za5 0.00040000 BTC • \$27.68	<b>To</b> 1 bc1qte4eg9vg0ghpechrhe6ftc8lz5*7fvy90yk8za5 0.00013228 BTC • \$9.15 2 bc1qtj39e75wajdlmu5ctp44zp3narg5gch3dxv9lv 0.00021631 BTC • \$14.97
ID: ada8-9cbd 1/31/2024, 14:34:10	
From bc1q-xldx To 2 Outputs 0.00040000 BTC • \$27.68 Fee 4.2K Sats • \$2.89	
<b>From</b> 1 bc1qwt2aztud5yypwvatr45a4yqwdlvf4q4rxzldx 0.05375181 BTC • \$3,719.95	<b>To</b> 1 bc1qtj39e75wajdlmu5ctp44zp3narg5gch3dxv9lv 0.00040000 BTC • \$27.68 2 bc1qwt2aztud5yypwvatr45a4yqwdlvf4q4rxzldx 0.05331004 BTC • \$3,689.38

15

## Common Scams and Frauds

### Typologies

- Impersonation Scams
- Investment Scams
- Romance Scams
- Pig Butchering

Sensitive but Unclassified/Business Confidential and Proprietary

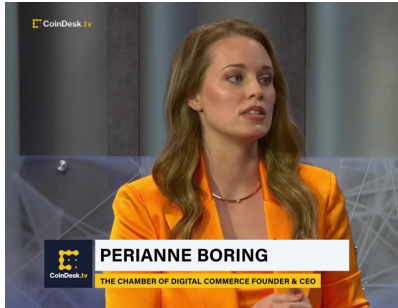
16





## Common Scams and Frauds

### Impersonation Scam



Impersonating a person or company using their Name, Image, or Likeness

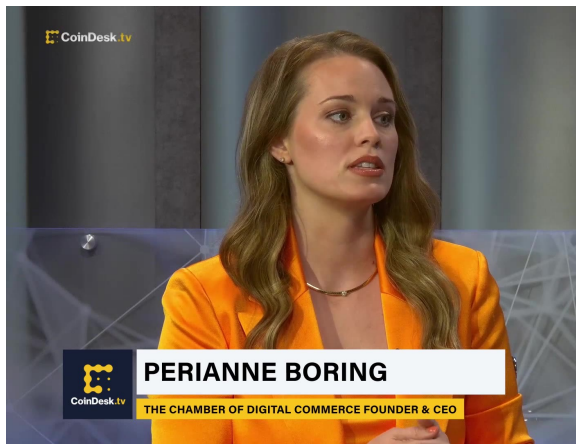
Real Names and photographs or real names and other photographs

Facebook, Instagram, Telegram, X (Twitter) etc, linked with a website and supporting online profile

Other fake accounts lending credibility



## Founder Digital Chamber of Commerce



The screenshot displays a search results page for 'Perianne Boring'. On the left, there are four profile cards, each with a profile picture, name, and an 'Add Friend' button. The profiles are: 1. Perianne Boring (Add Friend), 2. Perianne Boring (Bitcoin Mining at Chamber of Digital Commerce - Lives in Ne... (Add Friend), 3. Perianne Boring (Add Friend), 4. Boring Perianne (Lives in New York, New York (Add Friend). On the right, there is a vertical list of search results, each with a profile picture, name, and a brief bio or status. The results include: 1. perianne\_\_boring (Perianne Boring, Following), 2. perianne\_\_boring\_ (Perianne Boring), 3. paboring (Perianne Boring), 4. perianne\_boring1212 (perianne boring), 5. perianne\_boring2022 (Perianne boring), 6. periannedc\_org (Perianne Boring), 7. multiple543 (Perianne Boring legit investment platfo...).



Common Scams and Frauds

Investment Scams

Cryptocurrency Mining, FX Trading, Binary Options Trading, AI Supported Algorithms, Arbitrage, NFT, DeFi

Guaranteed results

Rug Pulls

Multiplier/Faucet Scams

Greed and Ignorance, Get Rich Quick

Sensitive but Unclassified/Business Confidential and Proprietary



Common Scams and Frauds

Romance Scams



Oldie but a goodie

Online dating apps increase reach and speed

COVID travel restrictions tilted field

Extensive and graphic online contact, psychological binding

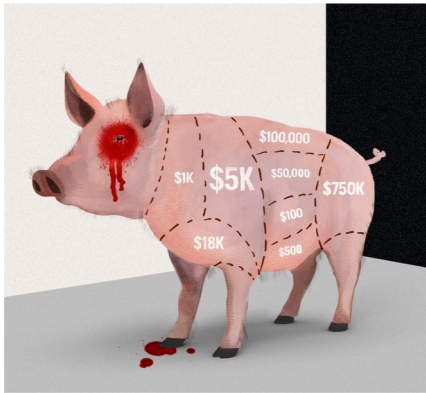
Travel expenses, legal expenses, lost credit cards

Sensitive but Unclassified/Business Confidential and Proprietary



## Common Scams and Frauds

### Pig Butchering



Romance plus Investment Scam = Super Scam

Dating site meeting

Sparking interest

Initial Investment gain and withdraw

More investments

Withdraw fees, taxes, etc, etc,

21

21



### Pig Butchering – Case Study



Dating App for High-Net-Worth individuals

Initial Connection and move to Whats App


Building rapport... BRB, I have to make a trade

Made \$10,000 in 20 minutes

Can you teach me? (Devil's greatest trick)


22

22

 <b>Pig Butchering – Case Study</b>	
Open Coinbase account and wire money into it	Initial trade, initial profit (15% in 30 min)
Sex and marriage (nudes)	Withdraw money back into bank account
More profits for him	Sense of loss created because of small amount
Time pressure not to miss opportunity	One more withdrawal, then immediate investing opportunity
Set up account on “investing site” (NYSE impersonator, including KYC)	Hook is set, wash, rinse, repeat
Transfer from Coinbase to investing site	

23

23

 <b>Pig Butchering – Case Study</b>	
Wire money, invest, profit, sex	Invests all loose money and salary
\$100k per day invested	Pivots to IRA, handles objections to penalties and taxes
Isolation – keep it a secret, don’t tell friends	Dad in hospital, cannot meet IRL
Coached on structuring wires and handling bank objections	Once account reaches \$4 million (investment plus gain) start withdrawal process
Planned meeting IRL	
Push to \$1 Million invested	Withdraw fee (\$250k) with time pressure

24

24

**V**

**Pig Butchering – Case Study**

More IRA withdrawals	Account frozen for ML concerns
Exceeded limits at Crypto exchanges	Needs money as sign of good faith there is no ML
Encouraged to borrow from friend to unlock her money	Pushed to get an online bank loan
Withdraw approved, triggers “audit” resulting in \$365k tax bill	Handling objections from friends
Borrowed more money, scammer pays last of money owed	More money sent, but to wrong wallet
	Technical fee to recover....

25

25

**V**

**Pig Butchering – Case Study**

Once cryptocurrency was received it was immediately transferred to another wallet

Three separate wallets were used to move funds, then the funds were lost in a mixer

Likely a team scam, formulaic process

Victim shaming, lack of familiarity with cryptocurrency, lack of jurisdiction and unlikely prosecution, little constituency or support from LE, affluent but not rich

\$1.75 Million Lost

26

26



## Fraud and Theft to Fund Weapons of Mass Destruction



Sensitive But Unclassified/Business Confidential and Proprietary

© REUTERS/KCNA

27

27



## North Korea Targeting Cryptocurrency Exchanges

UN is investigating 58 North Korean cryptocurrency thefts from 2017 to 2023 worth an estimated \$3 Billion.

Cryptocurrency exchanges are targeted using sophisticated social engineering and spear phishing techniques

North Korea makes around half of its foreign currency income from cyber attack on cryptocurrency

In 2022, a higher value of cryptocurrency assets were stolen by the DPRK than in any previous year

In 2023, North Korea stole \$600 Million in cryptocurrency (30% reduction since 2022)

28

28



## North Korea Cryptojacking

Mining cryptocurrency creates money out of thin air, but requires computing power and electricity

Cryptojacking is malware that steals a CPU's resources to mine cryptocurrency

Computers run slower and consume more electricity, but remain usable with data intact

Cryptojacking increased 400% in 2023, with more than 335 million incidents in first half of 2023 alone

Cisco's cloud security division reported Cryptojacking affecting 69% of its clients

We do not know the size and scale of this problem.

29

29



## Key Points

Cryptocurrency is here to stay

Cryptocurrency is value agnostic

Traditional criminal techniques with a new tool

Scams and fraud using cryptocurrency are on the rise

Hostile nation states leverage cryptocurrency to generate revenue

Education is key, take away criminal first mover advantage

Cryptocurrency is better experienced than explained. Get some.

30

30



**Discreet, bespoke solutions for  
appropriate clients**

**V VIGILANCE**

---

**Charles Finrock**

**Charles@vcci.io**

**703-980-5628**

© 2024 Finrock Group LLC, All Rights Reserved