Crystal Intelligence

Cryptocurrency AML, CFT and PF typologies

Nicholas Smart
Chief Intelligence Officer
8 Oct 2026

Laundering Plan – Key Points

- Several factors determine what currency, blockchain and protocols are taken by the criminal or terrorist organization.
- We can usefully hang these tactics under each element of the terrorism finance model: Raise, Store, Move, Spend.
- Using a specific tactic does not indicate one group or specific threat (i.e. TF, PF) – they are easily spoofed
- What kind of asset is wanted as an end state is the important detail, not where it started

Terminology and Attribution Problems

- Lots of vendor marketing phraseology out there
- “This must be x group because of y activity”
- Realistically, we are interested in the markers for any illicit activity
- Open, public blockchain means that terrorists learn from criminals, and vice versa
- SOME THINGS ARE JUST WRONG
  - All thefts are North Korea
  - All fraud is South Asian Compounds

On Chain Activity and Red Flags

- On-chain red flags are generally harder without attribution signals
- Behavioral indicators without attribution can work, but must be combined with off-chain signals like KYC/KYB

AML CFT and PF Stages

- Raise
- Pre Laundering Activity
- Laundering
- Conversion

Variation if AML/TF/PF

Predicate Crime

- Theft
- Fraud
- Fundraising
- Market Abuse Crimes

Raise

On-Chain Variation by Group

Placement, Layering and Integration

Pre Laundering → **Laundering** → **Conversion**

Tactics

Pre Laundering	Laundering	Conversion
Self Custodial Storage	Mixing	Licensed Exchange
Single Use Addresses	Own Token	Cash Service
Privacy Coins	Mule Accounts	

Variation if AML/TF/PF

Predicate Crime

- Theft
- Fraud
- Fundraising
- Market Abuse Crimes

Raise

On-Chain Variation by Group

Placement, Layering and Integration

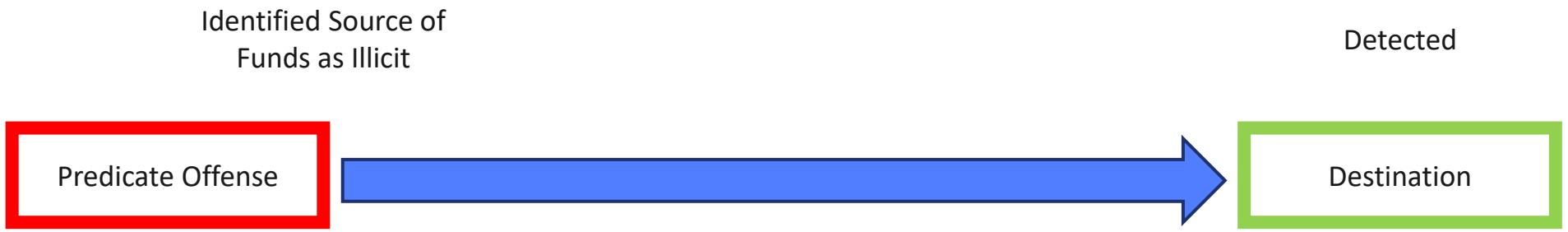
Pre Laundering	Laundering	Conversion
Tactics		
Self Custodial Storage	Mixing	Licensed Exchange
Single Use Addresses	Own Token	Cash Service
Privacy Coins	Mule Accounts	

Easy (-ier) to Observe → **More Difficult**


Predicate Offense
Destination

Identified Source of Funds as Illicit

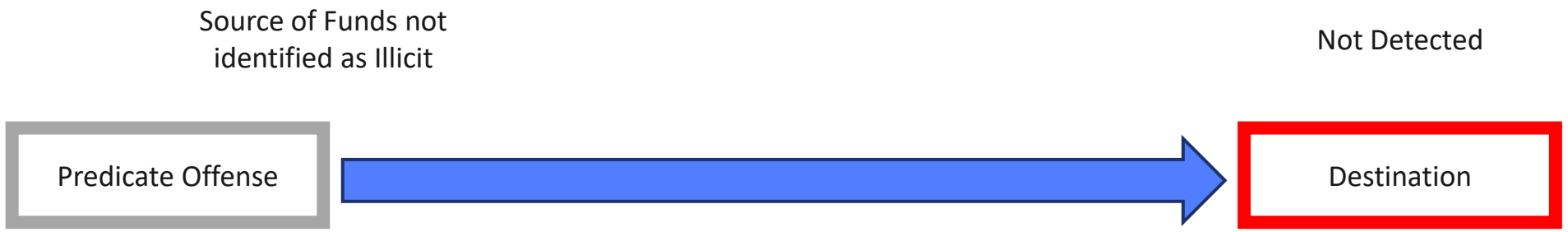


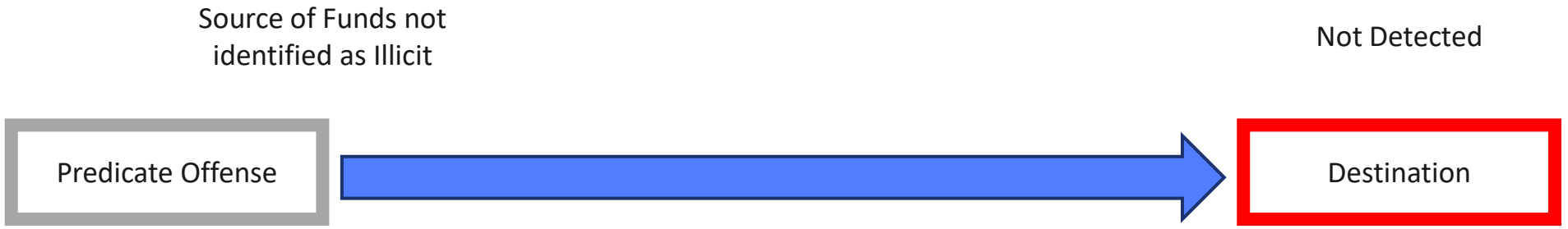

Identified Source of Funds as Illicit
Detected
Predicate Offense
Destination


Predicate Offense
Destination

Source of Funds not identified as Illicit




Source of Funds not identified as Illicit
Not Detected
Predicate Offense
Destination

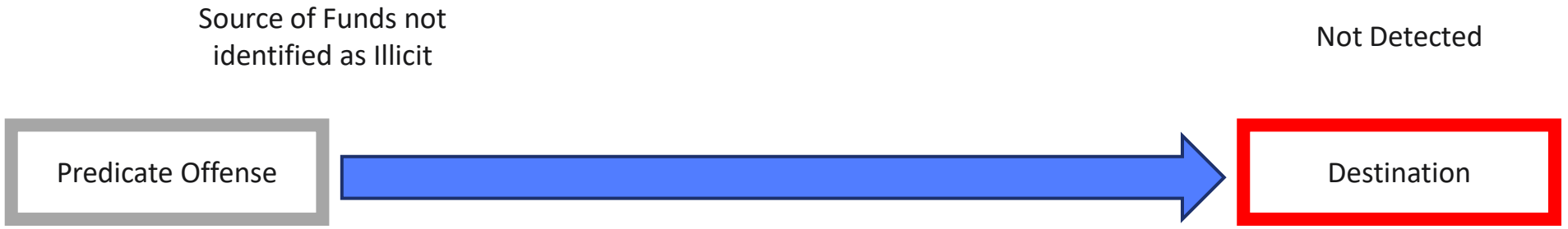


Why does KYT miss things?

Offense takes place off chain and uses on-chain to move funds

Crime has not been detected by KYT provider yet

Successful obfuscation/laundering process by criminals



Why does KYT miss things?

Offense takes place off chain and uses on-chain to move funds

Crime has not been detected by KYT provider yet

Successful obfuscation/laundering process by criminals

SO WHAT?

KYT is great, but not your only line of defense; KYC/B matters a lot too

Rechecking addresses is important as detections may be retrospective

Client Profiles count

Raise Funds

- Lots of possible predicates that overlap all typologies
  - Theft
  - Fraud
  - Market Manipulation
  - Fundraising

Typology	AML	PF	TF
Theft	X	X	X
Fraud	X	X	
Market Manipulation	X		
Fundraising		X	X

Raise: Fraud

- Cryptocurrency related fraud remains substantially high
- Beyond organised – *industrialised*
- Lots of mechanisms to convince people to send money

Raise: Fraud Indicators

- Interaction with other fraud addresses
- Receipt of fake tokens to deposit addresses
- Funds from Crypto ATM services
- Lack of clear economic purpose for account or transfer
- Website domains, tokens or key individuals reported on public warning lists

Raise: Theft

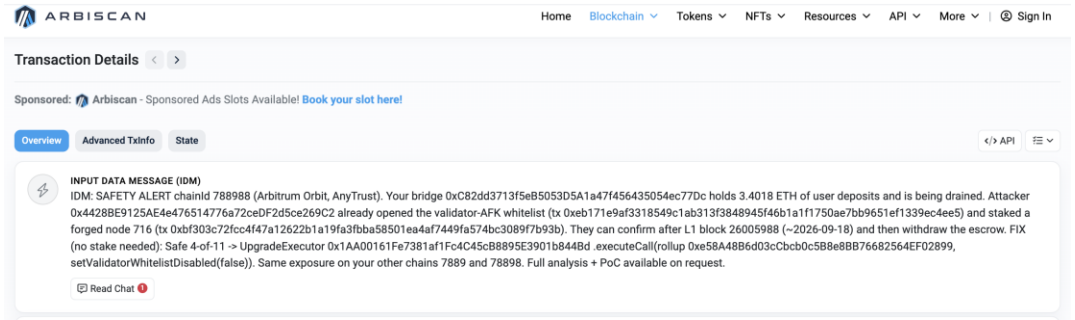
- Theft is a significant issue across AML/PF and even TF activity
- Funds have been stolen and used for proliferation by North Korean linked projects
- Technology makes funds hard to recover when stolen

Raise: Theft

- Theft is a significant issue across AML/PF and even TF activity
- Funds have been stolen and used for proliferation by North Korean linked projects
- Technology makes funds hard to recover when stolen and is often multi jurisdictional

Raise: Theft Indicators

- Large movement of funds from known service provider wallets
  - Drop to 0 is not uncommon – but not a guarantee
- Public announcement of thefts by service provider
- Funds typically travel directly to mixing/obfuscation services
- On-chain messages like the example





Raise: Fundraising

- Public donation campaigns are still common, but have generally have moved away from sharing a single QR code donation address unless solicited in privacy coins like Monero.
- Tend to now require contact with an organizer to get donation addresses.
- Rarely re-use wallet addresses and generate individual donation addresses.

Raise: Fundraising Indicators

- Small amounts transferred from lots of different sources, particularly different geographies for international terrorism.
- Public announcement of donations campaign may show the token type requested.
- On-chain exposure to other known Terrorism finance addresses.
- On-chain exposure to blocked funds (stablecoins)

Raise -> Pre Laundering Tactics

- Storage
  - Self Custody
  - Nested Services
  - Single Use Addresses
- Confiscation Resistance
  - Convert to Native Tokens
  - Convert to Resistant Tokens
  - Convert to Privacy Coins

Tactic	AML	PF	TF
Self Custody	X	X	X
Nested Services	X	X	X
Single Use Address	X		X
Conversion to Native Token	X	X	X
Conversion to Resistant Token	X	X	X
Convert to Privacy Coins	X	X	X

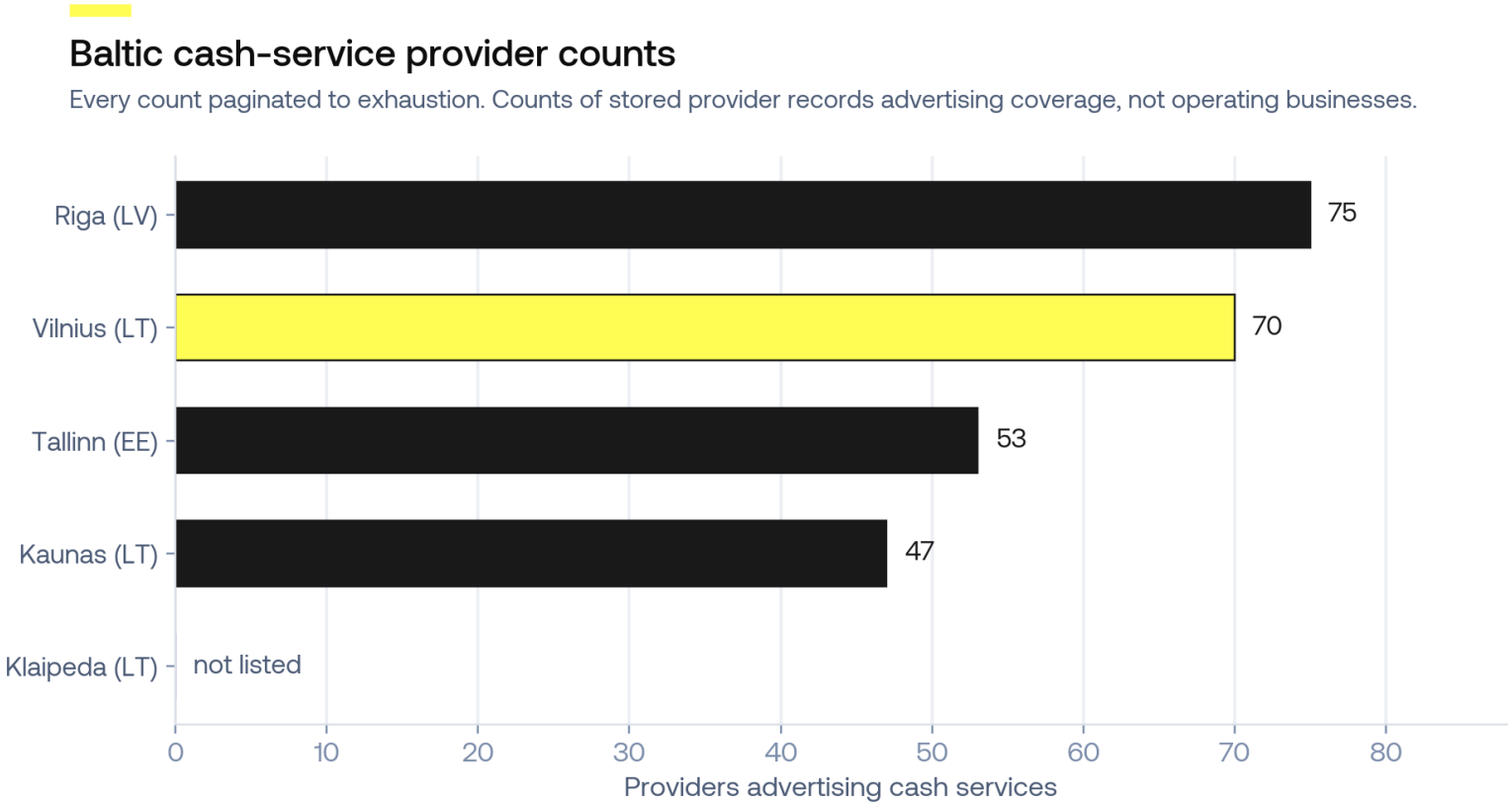
Laundering Tactics

- Decentralised Techniques
  - Cross Chain
  - Token Exchange
  - Staking
  - Own Token Issuance
- Mixing Services
- Instant Swap
- UTXO Methods
  - Coin Join
  - Peel Chain

Tactic	AML	PF	TF
Cross Chain	X	X	X
Token Exchange	X	X	X
Staking	X	X	
Own Token Issuance	X	X	
Mixing Services	X	X	X
Instant Swap	X	X	X
CoinJoin	X	X	X
Peel Chain	X	X	X

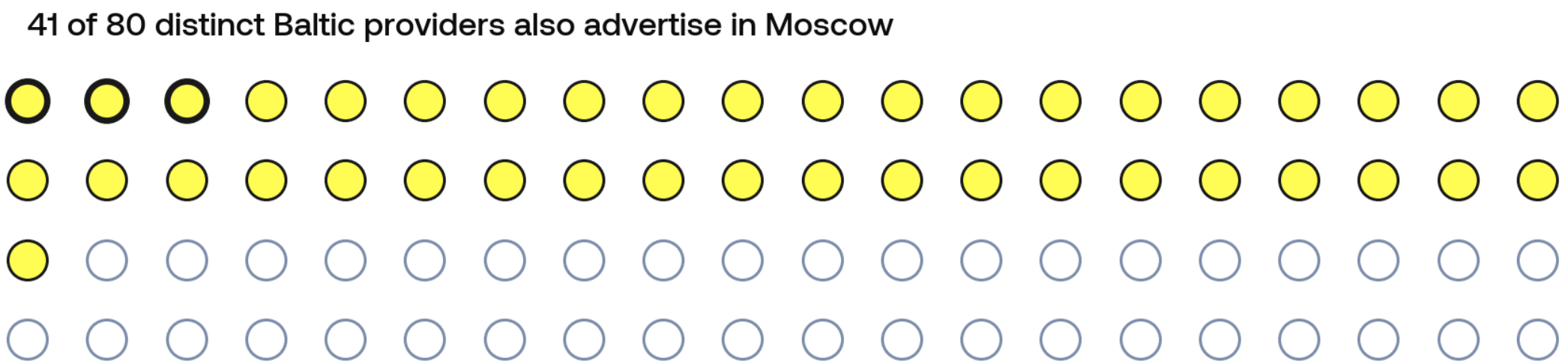
Unlicensed Exchanges

- Offshore License
- Wrong License
- No License



The Baltic provider population, by Moscow exposure

Each dot is one distinct provider across Riga, Vilnius, Tallinn and Kaunas.



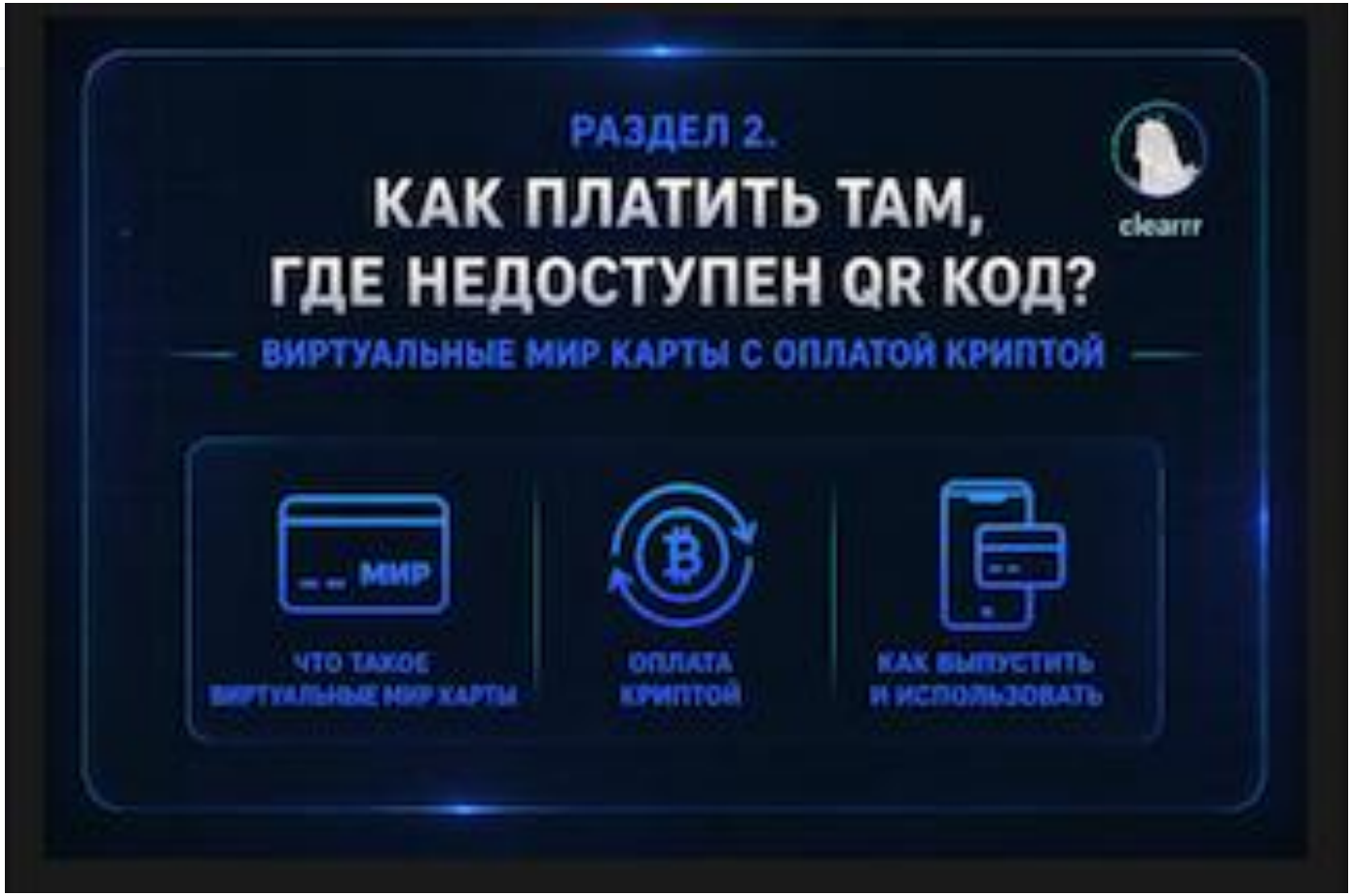
Bold outline: NordChange, ProstovCash and BaksMan — classified by Crystal as sanctions entities, EU Crypto Ban, riskscore 1.0.

Licensed Exchanges

- Money Mules
- Drop Account
- Intra Exchange Transfer

Laundering -> Conversion

- Crypto Debit Cards
- Cash Exchange
  - In Person
  - Courier
- Peer to Peer Transfer



“How to pay where a QR code isn't accepted?”

Red Flags – Consolidated Tactic Indicators (On Chain)

- Interaction with low reputation exchange or DeFi services
- Transaction originates from or is sent to a service in a high-risk jurisdiction with relevant exposure (TF, PF, Illicit Activity)
- Interaction with identified high risk or illicit services
- Broad geographic source for deposits
- Consistent high-volume deposits



Questions