



Technical Report and Findings

Re: Jean – Cryptocurrency Investigation

Analyst: M00872751

Organisation: CST3550

Date of Production: March 28th

Table of Contents

- 1. Investigation Overview**
 - 1.1 Purpose and Scope of the Investigation 2
 - 1.2 Data Types and Tools Utilised 2
- 2. Blockchain Forensics Analysis**
 - 2.1 Transaction Tracking Using Blockchain Explorer..... 2-3
 - 2.2 Obfuscation Techniques and Cross-Chain Analysis 3
 - 2.3 Visual Representations of Fund Movement..... 3
- 3. Attribution and Entity Identification**
 - 3.1 Wallet Address Attribution Methods 4
 - 3.2 Attribution Challenges and Mitigation 4
 - 3.3 Identified Entities and Roles 4
- 4. Recommendations and Conclusion**
 - 4.1 Strategies to Prevent Blockchain Misuse 5
 - 4.2 Summary of Findings and Legal Relevance 5
- Appendices**
 - A1. Blockchain Flow Diagrams 7
 - A2. Darknet Screenshots 8-9

1. Investigation Overview

1.1 Purpose and Scope of the Investigation

This investigation was initiated to analyse cryptocurrency activity linked to an individual, **Jean**, suspected of purchasing forged identity documents via a darknet vendor. The primary aim was to trace the origin and destination of related Bitcoin transactions and determine whether their structure, timing, and behaviour indicated criminal intent, including obfuscation or anonymity techniques.

The scope covered the full transaction lifecycle from **Jean's** acquisition of Bitcoin to the final payment to the suspected darknet wallet. A central focus was assessing whether the transferred values matched illicit marketplace prices and if specific wallet addresses could be reliably linked to real-world entities or defined roles in the transaction chain.

The investigation began when physical evidence containing the onion address (**7v6yjcmqem3jkj2.onion**) and the term "**Coingenie**" was anonymously deposited into a police post box. CCTV showed a male suspect placing the envelope, though identification was impossible due to a hoodie and balaclava. This evidence was referred to the Digital Forensics Investigation (DFI) unit.

1.2 Data Types and Tools Utilised

Initially, the term "**Coingenie**" was ambiguous. However, open-source intelligence later confirmed it was **Jean's** alias on **Bitcointalk.org**. Posts showed Jean seeking advice on web-based wallets and converting crypto to fiat indicating both anonymity concerns and financial intent.

Crystal Lite Blockchain Explorer was used to trace the transactions and verify hashes, timestamps, wallet linkages, and fees. **Microsoft Whiteboard** helped visualise the fund flow between wallets using colour-coded address diagrams. Additionally, **OSINT techniques** and screenshot archiving were applied to reinforce analysis and attribution. All processes followed digital forensic standards to preserve evidentiary integrity and maintain chain of custody.

2. Blockchain Forensics Analysis

2.1 Transaction Tracking Using Blockchain Explorer

The blockchain forensic analysis aimed to trace the flow of Bitcoin across key wallet addresses and identify behavioural patterns indicative of illegal activity. The investigation began by identifying Jean's suspected operational wallet referred to as the **Blue Address** (**1BsHJ7jErmkWqoSJNqPq72qMZzJ2wwKKNo**) and analysing its transaction history. This wallet received two separate payments: **0.8 BTC** and **0.2 BTC** on 16 and 17 February 2016, respectively. These payments originated from a secondary source, the **Green Address** (**12gTKgbd6QvAwIUuRKfcToq1aVjW8kD4y**), which was otherwise inactive, suggesting its sole purpose was to fund the **Blue Address**.

Following receipt, **Jean's Blue Address** transferred the exact same amounts 0.8 BTC and 0.2 BTC to a third address (**Grey Address: 1KEGwrH99rYJ6HG6VqAUcyEKpMwKLmF7zu**), which was later linked to the darknet vendor known as **DocsRus**. After network fees, the **Grey Address** received **0.7999 BTC** and **0.1999 BTC**, the total of **0.9998 BTC**. These values perfectly matched

the pricing structure for a forged **UK passport (0.8 BTC)** and **UK driver's license (0.2 BTC)** advertised on the associated marketplace, further affirming the illicit purpose of the transactions.

Each transaction was confirmed using Crystal Lite Blockchain Explorer, which enabled access to hashes, timestamps, fees, and transaction flows. The detailed traceability of these elements supports a timeline-based narrative consistent with deliberate financial structuring.

2.2 Obfuscation Techniques and Cross-Chain Analysis

An essential aspect of blockchain forensic work is identifying whether obfuscation tactics such as coin mixing, tumbling, or cross-chain token swaps have been used. These techniques are commonly applied to mask the link between sender and receiver.

In this case, no evidence was found of Jean employing such techniques. The transactions were straightforward **Bitcoin-to-Bitcoin** transfers with no intermediate conversions, smart contract interactions, or service provider redirections. However, the use of two split payments instead of a single 1 BTC transfer may represent an attempt at rudimentary obfuscation or mimic compliance with vendor-imposed payment rules. This layered structure can make it slightly more challenging to detect illicit activity during automated analytics, and as such, warrants investigative attention.

2.3 Visual Representations of Fund Movement

To support the analytical findings, visual tools were used to document transactional flows. **Microsoft Whiteboard** (Appendices) enabled the creation of a colour-coded transaction map, depicting three key wallet addresses **Green, Blue, and Grey** and their interactions. These visuals, included in the appendix, show not only directional fund transfers but also the exact transaction values and timing, clarifying the relationship between Jean and the darknet vendor.

The **Grey Address** exhibited further suspicious behaviour. It had received repeated payments from multiple, unrelated wallet sources usually in the **0.2 to 1 BTC** range consistent with the product pricing seen on the DocsRus marketplace. This repetitive, structured payment pattern suggests the address was used in an ongoing commercial capacity, acting as the endpoint for document purchases.

These combined insights technical traceability, behavioural patterning, and visual representation were essential in constructing evidence backed financial narrative. They helped corroborate Jean's role and provided clarity for further attribution efforts.

3. Attribution and Entity Identification

3.1 Wallet Address Attribution Methods

A key objective of this investigation was to determine ownership or control over the wallets involved in the transaction chain. Given that Bitcoin is pseudonymous by design, attribution efforts relied on the triangulation of behavioural patterns, transaction metadata, and open-source intelligence (**OSINT**). This process involved clustering wallet activity, assessing transaction flow, and comparing it with known marketplace data and publicly available digital footprints.

The **Green Address** (**12gTKgbd6QvAwiUuRKfcToq1aVjW8kD4y**) was identified as the original funding source. It issued two staged payments **0.8 BTC** and **0.2 BTC** to the **Blue Address** with no other outgoing activity, suggesting a dedicated, single use purpose. Its isolated function and tight transactional window imply that it may have been controlled by Jean, or a close associate tasked with transferring funds.

The **Blue Address** (**1BsHJ7jErmkWqoSJNqPq72qMZZj2wwKKNo**), acting as an intermediary, received exactly **1 BTC** before forwarding equivalent amounts to a third-party wallet. The sequential nature and lack of additional inbound or outbound activity further support the attribution of this address to Jean herself. It fits the behavioural profile of a temporary, user-controlled wallet created for a specific transaction sequence.

3.2 Attribution Challenges and Mitigation

Attribution was hindered by the absence of conventional identity markers such as IP addresses or verified exchange records due to the decentralised and pseudonymous nature of blockchain systems. Additionally, the marketplace (**7v6yjcmmqem3jkj2.onion**) was no longer online during the investigation, limiting live content validation.

To overcome these barriers, previously captured screenshots of the darknet site were used to confirm product listings and pricing. Further, the investigative team leveraged linguistic and contextual markers such as the email **docsrus@mail2tor.com** and phrases like “we will provide the best price we can for you” to connect the **Grey Address** (**1KEGwrH99rYJ6HG6VqAUcyEKpMwKLmF7zu**) to the vendor alias “**DocsRus**.”

A second challenge involved the ambiguous reference to “**Coingenie**” found in physical evidence. Through **OSINT** research, this was linked to Jean’s activity on **Bitcointalk.org**. Posts showed she was researching privacy-centric wallets and methods to convert crypto to fiat shortly before the transactions, indicating preparatory behaviour consistent with illicit activity.

3.3 Identified Entities and Roles

Three key addresses were attributed to distinct roles in the transaction chain:

- **Green Address:** Likely funding wallet, purpose-built or owned by Jean or an accomplice.
- **Blue Address:** Intermediary wallet under Jean’s control, used to forward funds.
- **Grey Address:** Recipient wallet belonging to DocsRus, a known darknet vendor.

Combined with timing, transaction values, and external data, these attributions support a strong evidential narrative linking Jean to the illegal purchase of forged documents.

4. Recommendations and Conclusion

4.1 Strategies to Prevent Blockchain Misuse

The results of this investigation underscore how blockchain's pseudonymous nature can facilitate the purchase of illicit goods, such as forged identification documents. To mitigate future misuse, the following multi-pronged strategies are recommended:

- **Mandatory Know-Your-Customer (KYC) Enforcement:** Regulatory authorities should require full **KYC** and Anti-Money Laundering (**AML**) compliance at all cryptocurrency entry points, including online exchanges and physical Bitcoin ATMs. Operators must collect verified user identification and maintain access-controlled video surveillance. This would allow investigators to trace criminal transactions more effectively and discourage misuse.
- **Real-Time Blockchain Monitoring Tools:** Law enforcement and financial institutions should implement blockchain analytics platforms capable of live monitoring. These tools must feature clustering algorithms, anomaly detection, wallet scoring, and transaction-pattern analysis. Integrating machine learning would further improve detection rates and predictive insights for criminal financial behaviour.
- **Vendor Wallet Blacklist Databases:** A globally accessible, continuously updated repository of suspicious wallet clusters should be maintained. These databases must interface with blockchain explorers and investigative platforms, enabling automated red flagging of addresses linked to darknet vendors, scams, or known threat actors.
- **Expanded OSINT and Cross-Domain Intelligence:** Blockchain data alone is often insufficient. Agencies should routinely merge wallet activity with online identities, forum posts, vendor listings, and communication traces. Open-source intelligence (**OSINT**) should be integrated into standard forensic workflows. Inter-agency and cross-border data-sharing protocols would further strengthen intelligence accuracy and attribution.
- **Training and Public Awareness:** Regular training for digital forensic analysts, law enforcement, and financial regulators should focus on evolving obfuscation techniques, cross-chain laundering, and forensic countermeasures. Public campaigns should also promote safe digital practices and encourage the reporting of suspicious crypto behaviour.

4.2 Summary of Findings and Legal Relevance

This investigation established a clear transactional link between Jean and the purchase of illicit forged documents via a darknet marketplace. Blockchain evidence was supported by visual wallet tracing and corroborated by Jean's alias "Coingenie" on Bitcointalk.org, which indicated intent and preparatory behaviour. Although the precise funding source remains unverified, the convergence of wallet flow, OSINT, and behavioural indicators builds a strong attribution profile.

This case demonstrates how blockchain forensic tools, when used in conjunction with intelligence analysis, can expose organised illicit activity and contribute directly to legal proceedings, regulatory enforcement, and the advancement of digital forensic methodology.

Appendices

A1. Blockchain Flow Diagrams

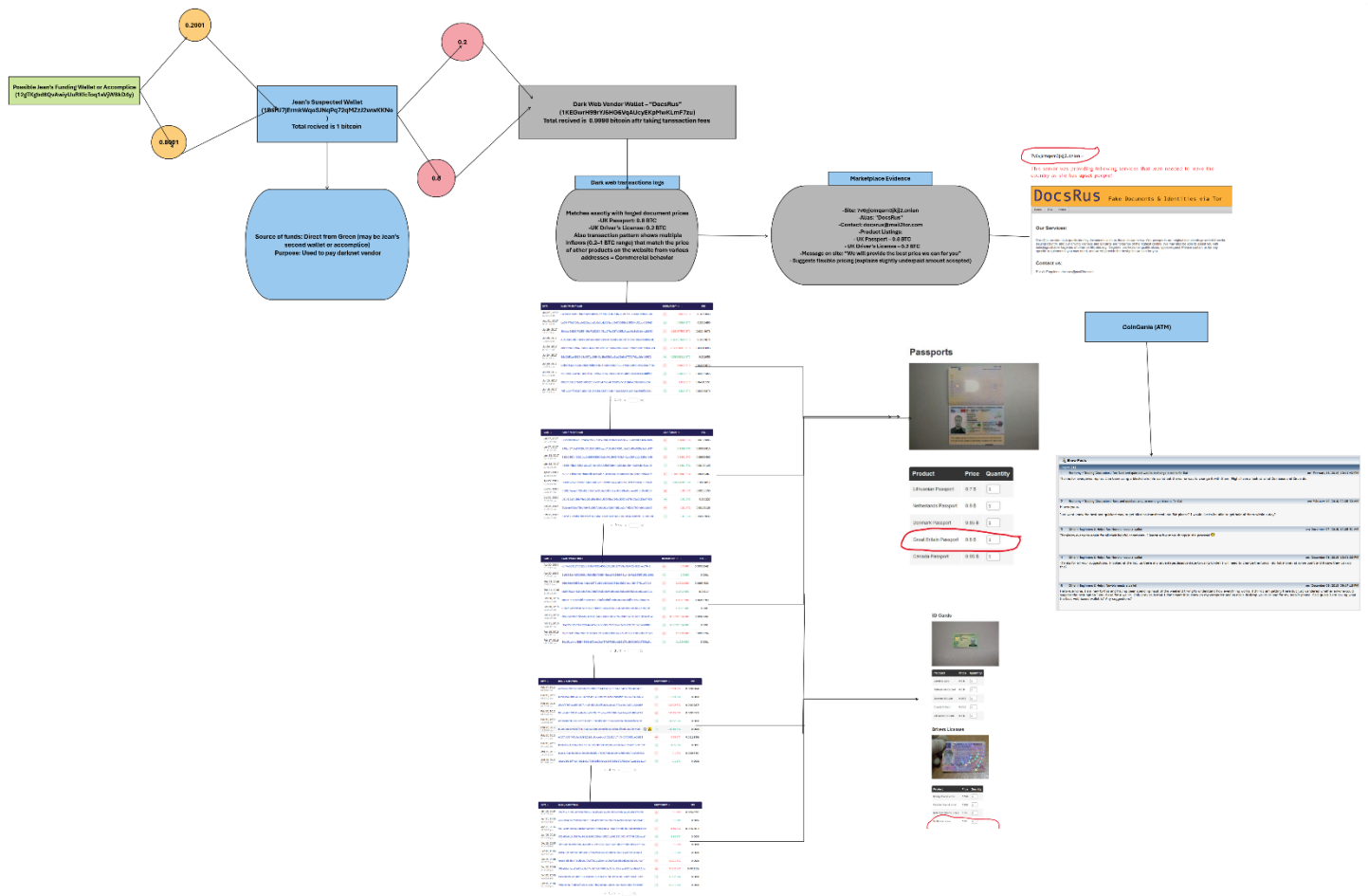


Figure 1: Blockchain Flow Diagrams

A2. Darknet webpage

7v6yjcmqem3jkj2.onion –

This server was providing following services that Jean needed to leave the country as she has upset people!

DocsRus

Fake Documents & Identities via Tor

Home FAQ Order


Our Services:

DocsRus provide high quality identity documents such as those shown below. Our passports are original documents provided from the issuing country, and our driving licenses and ID cards are forgeries of the highest calibre. We may also be able to assist you with indistinguishable forgeries of other certificates e.g. Degrees, professional qualifications, upon request. Please contact us for any specific requirements you may need, and we will provide the best price we can for you.

Contact us:

For All Enquiries: docsrus@mail2tor.com

Passports



Product	Price	Quantity
Lithuanian Passport	0.7 B	<input type="text" value="1"/>
Netherlands Passport	0.9 B	<input type="text" value="1"/>
Denmark Passport	0.85 B	<input type="text" value="1"/>
Great Britain Passport	0.8 B	<input type="text" value="1"/>
Canada Passport	0.95 B	<input type="text" value="1"/>

Figure 2: Darknet webpage 2/1

ID Cards



Product	Price	Quantity
Czech ID Card	0.6 B	<input type="text" value="1"/>
Netherlands ID Card	0.6 B	<input type="text" value="1"/>
Denmark ID Card	0.65 B	<input type="text" value="1"/>
French ID Card	0.65 B	<input type="text" value="1"/>
Lithuanian ID Card	0.5 B	<input type="text" value="1"/>

Drivers Licenses



Product	Price	Quantity
Norway Drivers License	0.35 B	<input type="text" value="1"/>
Denmark Drivers License	0.25 B	<input type="text" value="1"/>
Netherlands Drivers License	0.3 B	<input type="text" value="1"/>
UK Drivers License	0.2 B	<input type="text" value="1"/>

DocsRus 7v6yjcmgqnsjkj2.onion

Figure 3: Darknet webpage 2/2