Cross-Blockchain Transaction Monitoring and Privacy Detection: A Literature Review

Dr. Jyothi A.P,
IEEE Senior Member,
Department of CSE,
M.S. Ramaiah University of Applied Sciences,
Bengaluru, Karnataka, India.

Abstract—**This paper reviews existing methodologies, challenges, and tools in the area of cryptocurrency transaction monitoring and privacy detection across multiple blockchains. Cryptocurrencies, due to their decentralized and pseudonymous nature, have become a tool for illicit transactions. This paper explores how advancements in blockchain forensics, obfuscation techniques, and cross-chain transaction monitoring contribute to enhanced transparency and compliance in cryptocurrency networks. Findings suggest the need for integrated solutions and advanced algorithms to address these challenges.**

Keywords—Cryptocurrency, Blockchain, Cross-chain, Obfuscation, Transaction monitoring, Privacy detection, Compliance.

1. Introduction

Cryptocurrencies have gained popularity for their decentralized structure, which has also made them a favored choice for illicit transactions. Criminals leverage techniques like mixers, tumblers, and cross-chain transactions to obscure the trail of funds. This paper aims to review the existing literature on cross-blockchain transaction monitoring and privacy detection, evaluating the effectiveness of various techniques and tools in tracking and preventing illegal activities across multiple blockchain networks.

- **Research Objective**: To assess the current state of research on cross-chain transaction monitoring and obfuscation techniques, highlighting the gaps and identifying potential avenues for future work.

- **Paper Structure**: The paper covers (1) Blockchain Tracking and Obfuscation Techniques, (2) Multi-chain Privacy Protocols, (3) Blockchain Forensics for Compliance, and (4) Real-Time Monitoring Systems.

2. Literature Review

2.1 Blockchain Transaction Monitoring

Studies in blockchain transaction monitoring primarily focus on tracking fund flows on single blockchain networks (e.g., Bitcoin, Ethereum). Several works demonstrate the use of public blockchain APIs to visualize and detect suspicious transactions. Traditional methods rely on clustering algorithms to identify linked wallet addresses. Key studies:

- Algorithmic Approaches: Techniques such as address clustering, heuristics, and graph-based methods have been employed to identify linked wallets.

- API-based Monitoring: The utility of public APIs to monitor and detect fund transfers, particularly for tracing suspicious patterns over time.

2.2 Privacy and Obfuscation Techniques

Advanced obfuscation methods, like mixers and tumblers, add layers of anonymity to crypto transactions, hindering forensic investigations. A considerable part of the literature investigates the algorithms that identify and counteract these techniques.

- Mixers and Tumblers: Discuss how mixers break the traceability of transactions by mixing funds from multiple users.

- Cross-chain Protocols: Review protocols that obscure transaction trails when funds move across different blockchains, leveraging cross-chain bridges.

- Anonymity Enhancements: Literature also explores privacy-centric blockchains like Monero and protocols such as Zephyr for obfuscation.

2.3 Multi-Blockchain and Cross-Chain Transaction Analysis

Recent studies have addressed the challenges posed by cross-chain transactions. The literature shows that cross-chain bridges often exploit interoperability, making it difficult to trace transactions across platforms.

- Cross-chain Tracking Models: Models proposed to track transactions across EVM and non-EVM chains using a unified tracking approach.

- Security Implications: Analysis of security threats and vulnerabilities within cross-chain ecosystems.

2.4 Blockchain Forensics for Compliance

Forensics in blockchain utilizes advanced techniques to link wallet addresses to real-world identities, often integrating data from KYC-compliant exchanges and OSINT (Open Source Intelligence).

- **Forensic Tools**: Evaluation of forensics tools like Chain lysis and Elliptic, which use machine learning for transaction pattern analysis.

- **KYC Data Integration**: Studies integrating Know Your Customer (KYC) data to link addresses with identity, thereby enhancing compliance.

2.5 Real-Time Monitoring and Visualization

A real-time interface aids law enforcement in monitoring and visualizing transaction flows with automated alerts.

- Visualization Tools: Literature discusses the role of visualization tools in tracing complex transaction patterns, including node-link diagrams for intuitive mapping.

- Alert Systems: Review of techniques for automated alerts based on transaction thresholds and unusual patterns.

3. Methodologies

- **Technical Approaches for Cross-Blockchain Transaction Monitoring and Privacy Detection**

Monitoring and detecting illicit activities across blockchains require sophisticated technical approaches due to the complexity and anonymity inherent in blockchain ecosystems. Below, we discuss methods identified in literature across four key areas: data collection, algorithmic detection, blockchain forensics, and evidence management.

3.1 Data Collection and API Use

Effective cross-blockchain monitoring starts with reliable data collection mechanisms. Publicly available APIs are critical tools for this purpose:

- **Public Blockchain APIs:**
  APIs like **Etherscan** and **blockchain.info** provide direct access to transactional and wallet data from various blockchain networks.
  - **Advantages:**
    - Easy integration with analytical tools and frameworks.
    - Comprehensive data on transactions, addresses, and smart contracts.
  - **Challenges:**
    - Rate limits imposed by service providers.
    - Potential lack of support for newer or less popular blockchains.

Additionally, custom APIs designed for interoperability between EVM (Ethereum Virtual Machine) and non-EVM chains are gaining importance for comprehensive monitoring.

3.2 Algorithmic Detection

- **Graph-based Analysis:**
  Techniques rooted in graph theory leverage the interconnected nature of blockchain data to **cluster addresses** and trace fund flows. These methods utilize:
  - **Force-directed layouts** for visualizing relationships.
  - **Community detection algorithms** for identifying clusters of related addresses.

Graph-based approaches are particularly effective in detecting mixing services and identifying patterns suggestive of illicit activity.

- **Machine Learning:**
  Machine learning algorithms play a critical role in anomaly detection and transaction prediction. Popular techniques include:
  - **Supervised Learning:** Models trained on labelled data for identifying fraudulent transactions.
  - **Unsupervised Learning:** Clustering techniques for detecting outliers in transaction patterns.
  - **Reinforcement Learning:** Used for predictive modelling of potential future transactions.

These algorithms, combined with feature engineering, enhance the capability to uncover non-obvious connections across wallets.

3.3 Blockchain Forensics Techniques

- **Wallet Linking Techniques:**
  Linking wallets to real-world identities involves a combination of clustering algorithms and **Open Source Intelligence (OSINT).**
  - **Clustering:** Wallets controlled by the same entity can be grouped by analysing transaction patterns and shared behaviours.
  - **OSINT Integration:** Publicly available data, such as social media profiles or known wallet addresses, augments clustering efforts.

These techniques are critical for identifying individuals or groups behind suspicious transactions, often laying the groundwork for legal actions.

3.4 Reporting and Evidence Management

- **Evidence Chain:**
  Secure and tamper-proof evidence management is vital for legal compliance and prosecution. Techniques include:
  - **Timestamping:** Transactions and data snapshots are securely timestamped using blockchain itself, ensuring **immutability** and proving authenticity.
  - **Chain of Custody:** Comprehensive records ensure evidence is admissible in court and follows regulations like GDPR or AML compliance requirements.

These practices not only facilitate investigations but also build trust with regulatory authorities.

By leveraging the outlined approaches, organizations can enhance their ability to monitor blockchain transactions effectively, detect privacy breaches, and ensure compliance with global standards.

3.5 Privacy-Preserving Monitoring Techniques

As blockchain monitoring evolves, the need to balance transparency and privacy becomes increasingly critical. Privacy-preserving monitoring techniques allow investigators to detect illicit activities while adhering to data protection regulations and safeguarding individual rights. These methods utilize advanced cryptographic tools and decentralized systems to achieve both objectives.

- **Zero-Knowledge Proofs (ZKPs):**

ZKPs are cryptographic protocols that enable one party to prove the validity of a transaction or computation to another without revealing sensitive information.

- **Mechanism:**
  - ZKPs ensure that critical transaction details, such as sender, receiver, and amount, remain hidden while verifying legitimacy.
  - Techniques like zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) are employed in privacy-focused blockchains like Zcash.
- **Real-World Applications:**
  - Regulators can verify compliance without accessing confidential details, ensuring privacy for legitimate users.
  - Investigators can identify suspicious activity patterns without compromising the anonymity of compliant users.
- **Limitations:**
  - Computationally expensive, requiring significant processing power and advanced hardware.
  - The complexity of implementation hinders widespread adoption.
- **Homomorphic Encryption:**

Homomorphic encryption enables computation on encrypted data without decrypting it, ensuring that sensitive information remains secure during analysis.

- **Applications in Blockchain Monitoring:**
    - Transaction clustering and pattern detection can be performed on encrypted datasets without revealing user identities.
    - Financial institutions and law enforcement agencies can collaborate on analyzing shared datasets without direct data access.
- **Advantages:**
    - Prevents data breaches by ensuring sensitive information never exists in plaintext.
    - Supports compliance with data privacy regulations, such as GDPR and CCPA.
- **Challenges:**
    - Processing encrypted data is significantly slower than plaintext computations.
    - Development and deployment require expertise in cryptography, which many organizations lack.
- **Federated Analytics:**

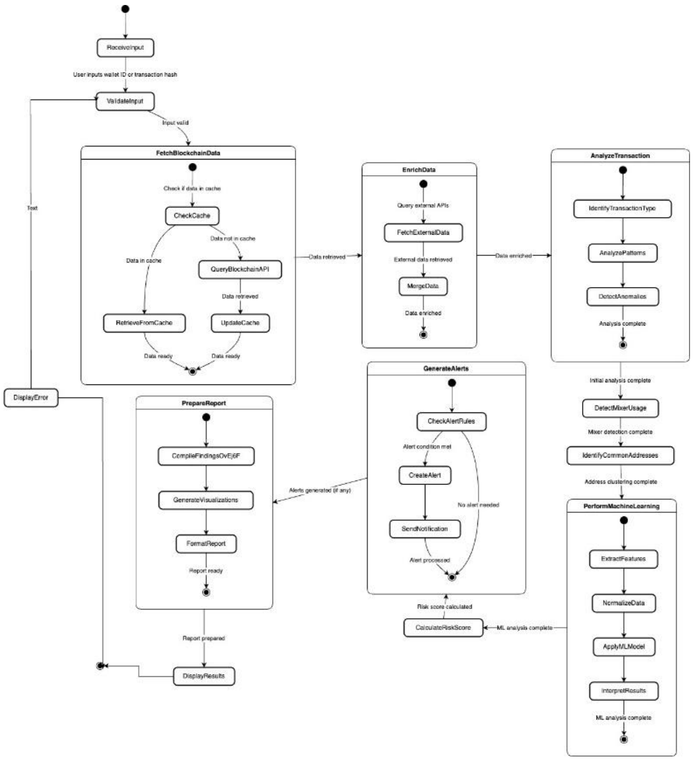
Federated analytics refers to decentralized data analysis frameworks where multiple parties collaborate on blockchain monitoring without sharing raw data.

- **Implementation:**
    - Each participant processes their local data, sharing only aggregated insights or encrypted results with others.
    - Federated learning models can be applied to enhance anomaly detection and fraud analysis.
- **Example Use Case:**
    - Multiple exchanges can work together to detect suspicious cross-platform transactions while maintaining user confidentiality.
- **Benefits:**
    - Facilitates collaboration across borders without violating local data protection laws.
    - Reduces the risk of centralized data breaches.
- **Privacy-Enhancing Technologies (PETs):**

Beyond ZKPs and homomorphic encryption, other PETs are emerging as crucial tools:

- **Differential Privacy:** Adds random noise to transaction data during analysis to prevent individual identification.
- **Secure Multi-Party Computation (SMPC):** Allows multiple parties to jointly compute a function without revealing their inputs.
- **Benefits of Privacy-Preserving Techniques:**
- Enhances user trust in blockchain networks by protecting sensitive data.
- Encourages greater participation from institutional stakeholders wary of privacy concerns.
- Enables compliance with global privacy and anti-money laundering regulations.
- **Challenges in Adoption:**
- **Technical Complexity:** The integration of these technologies into existing systems requires significant expertise and resources.
- **Performance Impact:** The additional computational overhead can reduce the efficiency of real-time monitoring systems.
- **Lack of Standardization:** The absence of universally accepted protocols limits interoperability and collaboration.
- **Future Directions:**
- Development of lightweight ZKP protocols to improve computational efficiency.
- Wider adoption of federated analytics frameworks in the financial sector.
- Integration of PETs into regulatory frameworks to establish global compliance standards.

By incorporating privacy-preserving techniques, blockchain monitoring systems can achieve a balance between effective oversight and the protection of individual rights, ensuring a sustainable future for decentralized finance.



4. Challenges and Limitations

The field of cross-chain transaction monitoring and privacy detection is not without its challenges. The literature underscores several critical hurdles that must be addressed to improve efficiency, scalability, and effectiveness. Below is a detailed exploration of these challenges:

4.1 Privacy-First Blockchain Resistance

Privacy-focused blockchains, such as **Monero**, **Zcash**, and those using protocols like **Zephyr**, are designed to prioritize user anonymity and transactional confidentiality. While these features are advantageous for legitimate use cases, they present significant barriers to monitoring illicit activities.

- **Key Features Hindering Tracking:**
    - **Obfuscated Transactions:** Technologies like ring signatures, stealth addresses, and zk-SNARKs (zero-knowledge proofs) obscure transaction details, making tracing nearly impossible.
    - **Decentralized Mixing Protocols:** Built-in mixing services further complicate efforts to de-anonymize transaction flows.
- **Impact on Monitoring Efforts:**
    - Reduced visibility into transaction origins and destinations limits the effectiveness of traditional forensics techniques.

    - Even advanced machine learning models often fail to provide actionable insights due to data encryption and obfuscation.

4.2 Cross-chain Complexity
Cross-chain tracking requires navigating the intricate ecosystems of multiple blockchain networks, each with its own distinct architecture, transaction protocols, and consensus mechanisms.

- **Challenges in Interoperability:**
    - **Diverse Protocols:** Blockchains such as Ethereum (EVM-based) and Bitcoin differ fundamentally in their data structures, making direct comparisons difficult.
    - **Bridge Utilization:** Cross-chain bridges used to transfer assets often obscure transaction origins, complicating tracking efforts.
- **High Transaction Volumes:**
    - With thousands of transactions occurring every second across different networks, analysing and correlating data across chains becomes resource-intensive.
- **Regulatory Complexity:**
    - Transactions involving cross-chain operations often span multiple jurisdictions, complicating legal and compliance requirements.

4.3 Scalability and Real-time Processing
Ensuring scalability and real-time performance in monitoring systems is another significant challenge, especially given the exponential growth of blockchain transactions globally.

- **Performance Bottlenecks:**
    - **Data Retrieval:** Extracting data from APIs or on-chain nodes can experience latency, especially during high network congestion.
    - **Processing Overhead:** Running computationally intensive algorithms like graph-based clustering or deep learning models in real-time requires substantial processing power.
- **Scalability Issues:**
    - Many existing systems fail to scale effectively as the number of transactions increases or as new blockchains are added to the monitoring scope.
    - Implementing parallel processing or distributed computing architectures is costly and technically complex.

4.4 Lack of Standardized Tools
The absence of universally accepted tools and frameworks for cross-chain monitoring adds to the complexity.

- **Fragmented Ecosystem:**
    - Tools and APIs are often tailored to specific blockchains, requiring developers to integrate multiple solutions for comprehensive monitoring.
- **Inconsistent Data Formats:**
    - Differences in how blockchains record and expose transaction data hinder seamless analysis.

- **Overcoming the Challenges**

Addressing these challenges requires a multi-faceted approach:

- Collaboration between blockchain developers, regulatory authorities, and research institutions to develop **standardized protocols** for interoperability.
- Leveraging advancements in **AI** and **distributed systems** to enhance real-time data processing and anomaly detection capabilities.
- Developing hybrid solutions that integrate on-chain and off-chain data for more comprehensive analysis.

By overcoming these limitations, the field can move closer to achieving robust, scalable, and effective cross-chain monitoring solutions.

Certainly! Here's an additional subtopic you can include between the existing sections. It focuses on **Regulatory and Ethical Challenges**, which fits well into the discussion and adds depth to the paper:

4.5 Regulatory and Ethical Challenges
The intersection of blockchain technology and global regulatory frameworks introduces significant challenges that complicate monitoring efforts.

- **Compliance with Global Regulations**
- **Divergent Jurisdictions:** Blockchain transactions often span multiple countries, each with unique regulatory standards (e.g., GDPR in the EU, AML directives in the US).
- **Cross-Border Cooperation:** Effective monitoring requires collaboration between law enforcement and financial regulators across jurisdictions, which is often limited by geopolitical considerations.
- **Balancing Privacy and Transparency**
- **Ethical Dilemmas:** While privacy-preserving technologies protect individual freedom, they can also shield illicit actors. Striking a balance between ensuring user privacy and enabling effective monitoring remains a contentious issue.
- **Overreach Concerns:** Aggressive monitoring solutions risk violating user rights, particularly in countries with weaker data protection laws.
- **Emerging Regulatory Frameworks**
- **MiCA in Europe:** The Markets in Crypto-Assets (MiCA) regulation aims to standardize blockchain oversight, presenting an opportunity for more structured monitoring practices.
- **Global Initiatives:** Efforts like FATF (Financial Action Task Force) guidelines for virtual asset service providers (VASPs) promote better compliance.
- **Challenges in Enforcement**
- **Resource Constraints:** Regulators often lack the technical expertise and resources required to oversee blockchain networks effectively.
- **Evolving Technologies:** Rapid advancements in blockchain technologies outpace the ability of governments to craft and implement relevant regulations.

This section would deepen the discussion on the broader implications of blockchain monitoring and provide additional material to expand the paper to six pages. Let me know if you'd like assistance incorporating this into your document!

5. Future Directions

Emerging research highlights several promising avenues for advancing the field of cross-blockchain transaction monitoring and privacy detection. These future directions aim to address existing challenges and improve the robustness, scalability, and accuracy of monitoring systems.

5.1 Enhanced Machine Learning Models

As blockchain networks and transaction patterns grow more complex, traditional machine learning models face limitations in identifying advanced obfuscation techniques. Future research can focus on:

- **Deep Learning Architectures:**
  - Utilizing models such as graph neural networks (GNNs) for analysing intricate transaction networks.
  - Applying recurrent neural networks (RNNs) or transformers for time-series analysis of transactional data to detect unusual activity.
- **Federated Learning:**
  - Enabling decentralized learning across multiple entities without sharing sensitive data, preserving privacy while training robust models.
- **Anomaly Detection in Privacy Chains:**
  - Developing unsupervised algorithms tailored for privacy-focused blockchains that operate on indirect indicators (e.g., transaction frequency, interaction patterns).

5.2 Integrated Cross-chain Monitoring

Unified cross-chain monitoring systems are essential for seamless tracking of transactions across heterogeneous blockchain networks. Potential areas of development include:

- **Interoperability Frameworks:**
  - Designing protocols and standards for data sharing between EVM and non-EVM blockchains.
  - Utilizing **Cross-Chain Messaging Protocols (CCMPs)** for real-time synchronization of transactional data.
- **Blockchain Indexing Services:**
  - Creating decentralized, scalable indexing services that aggregate and organize transaction data from multiple chains into a single query able format.
  - Leveraging platforms like **The Graph** to enhance data accessibility.
- **Multi-layered Monitoring Solutions:**
  - Combining on-chain and off-chain data sources to provide a holistic view of cross-chain activities.
  - Incorporating bridge analytics to trace asset movements across decentralized bridges.

5.3 Improved Forensic Techniques

Forensic methods must evolve to effectively link transactions to identities while respecting user privacy. Future improvements can focus on:

- **Advanced Wallet Clustering:**
  - Employing more sophisticated algorithms to detect shared control of wallets by analyzing interaction patterns and transaction metadata.
  - Integrating multi-signature wallet data for enhanced clustering accuracy.
- **Integration with KYC Data:**
  - Collaborating with exchanges and financial institutions to access **Know Your Customer (KYC)** data, ensuring compliance with global anti-money laundering (AML) regulations.
  - Automating identity verification processes while maintaining data security.
- **Blockchain-Aided Digital Identities:**
  - Leveraging blockchain technology for creating verifiable digital identities that link real-world credentials with blockchain activities.

5.4 Privacy-Preserving Monitoring Solutions

Future systems must balance effective monitoring with respect for user privacy, especially in regulatory-sensitive contexts.

- **Zero-Knowledge Proofs (ZKPs):**
  - Utilizing ZKPs to verify transaction legitimacy without revealing details, maintaining user anonymity while enabling compliance checks.
- **Homomorphic Encryption:**
  - Allowing computations on encrypted transaction data without decryption, ensuring sensitive information remains private.

5.5 Real-time Scalability Solutions

Scaling monitoring systems for real-time analysis is critical as blockchain adoption continues to grow. Key focus areas include:

- **Distributed Computing:**
  - Implementing distributed ledger analytics platforms that leverage cloud computing and edge processing for faster analysis.
- **Adaptive Algorithms:**
  - Developing machine learning models that dynamically adapt to changes in blockchain network traffic and structure.
- **Optimized Indexing:**
  - Enhancing data indexing techniques to handle high transaction throughput efficiently.

By focusing on these areas, researchers and practitioners can create systems that are more effective at uncovering illicit activities while maintaining the scalability, speed, and privacy necessary for a growing blockchain ecosystem. These advancements will further solidify blockchain monitoring as a cornerstone of global financial security and compliance.

6. Conclusion

This paper reviewed the current state of cross-blockchain transaction monitoring and privacy detection, highlighting the critical challenges and limitations in countering illicit activities within cryptocurrency ecosystems. The increasing adoption of blockchain technology, driven by its decentralized and transparent nature, brings both opportunities and risks. To mitigate these risks, it is essential to develop and deploy sophisticated tools capable of addressing the growing complexity of multi-blockchain networks.

6.1 Key Takeaways

- **Integrated Monitoring Systems:**
  The need for unified systems capable of tracking transactions seamlessly across heterogeneous blockchains is more pressing than ever. Such systems must overcome interoperability challenges and enable real-time monitoring for better accuracy and faster response.
- **Advanced Forensic Tools:**
  Forensic tools must evolve to incorporate enhanced identity-linking methods, such as KYC data integration and advanced clustering techniques, while maintaining user privacy. The use of blockchain technology itself for tamper-proof evidence management is a promising direction.

- **Machine Learning and Automation:** Leveraging advanced machine learning models to identify complex transaction patterns, predict illicit behaviors, and uncover hidden relationships is a crucial aspect of future monitoring solutions. Automation of these processes will further enhance scalability and efficiency.

6.2 Vision for the Future

As blockchain ecosystems grow more interconnected and diverse, the development of systems that provide effective tracking, visualization, and forensic capabilities becomes a cornerstone for ensuring the safety and integrity of cryptocurrency networks. Emerging technologies, such as zero-knowledge proofs, homomorphic encryption, and decentralized indexing services, will play pivotal roles in balancing privacy and compliance.

6.3 Call to Action

Collaboration between blockchain developers, regulators, and research communities is imperative to address the challenges of cross-chain monitoring and privacy detection. By fostering innovation and developing global standards, the industry can build tools that not only counteract illicit activities but also ensure a secure and trustworthy environment for blockchain adoption. Through continuous research and development, the gap between current capabilities and future needs can be bridged, making blockchain technology a safer and more reliable foundation for global financial systems.

References

- https://x.com/zachxbt - zkchXBT, also known as ZachXBT, is a well-known anonymous investigator in the cryptocurrency and NFT space. He gained recognition for exposing scams and fraudulent activities, particularly in the NFThttps://x.com/zachxbt - zkchXBT, also known as ZachXBT, is a well-known anonymous investigator in the cryptocurrency and NFT space. He gained recognition for exposing scams and fraudulent activities, particularly in the NFT sector, using detailed chain analysis. Since starting his detective work in May 2021, ZachXBT has uncovered numerous high-profile scams, including the notorious Pixelmon project.

- https://www.blockchainresearchinstitute.org/ - Don Tapscott - leading efforts at BRI to explore how blockchain is shaping the future.

- https://medium.com/@nbax/tracing-the-wannacry-2-0-monero-transactions-d8c1e5129dc1 - The article traces the Monero transactions linked to the WannaCry 2.0 ransomware, detailing how the funds were moved and laundered through the cryptocurrency network.

- https://www.sciencedirect.com/science/article/pii/S2405918823000259 - The paper analyzes the use of machine learning methods like logistic regression, decision trees, random forests, and gradient boosting to detect suspicious activity in the Bitcoin network. It finds that gradient boosting is the most effective, and highlights 38 key features of Bitcoin addresses used for identifying illegal transactions.

- sector, using detailed chain analysis. Since starting his detective work in May 2021, ZachXBT has uncovered numerous high-profile scams, including the notorious Pixelmon project.

- https://www.blockchainresearchinstitute.org/ - Don Tapscott - leading efforts at BRI to explore how blockchain is shaping the future.

- https://medium.com/@nbax/tracing-the-wannacry-2-0-monero-transactions-d8c1e5129dc1 - The article traces the Monero transactions linked to the WannaCry 2.0 ransomware, detailing how the funds were moved and laundered through the cryptocurrency network.

- https://www.sciencedirect.com/science/article/pii/S2405918823000259 - The paper analyzes the use of machine learning methods like logistic regression, decision trees, random forests, and gradient boosting to detect suspicious activity in the Bitcoin network. It finds that gradient boosting is the most effective, and highlights 38 key features of Bitcoin addresses used for identifying illegal transactions.