Blockchain and Cyber-Security: the Opportunity to Develop a National Data Analysis Platform to Ensure National Security and Financial Stability

Bogdan VACUSTA[1], Constantin NICA[2]
[1]Accredited Counter Fraud Manager, UK Counter Fraud Professional Accreditation Board
[2]Cybersecurity Researcher
vacusta.bogdan@gmail.com, nightsim@proton.me

Abstract: Worldwide media is reporting an alarming increase in cyber-attacks targeting critical infrastructure systems, posing a significant threat to national security and financial stability. The tight dependency between various systems like financial institutions, companies supplying assorted services, healthcare or education, makes cyberattacks, a formidable weapon that can affect nation-wide infrastructures. Illicit activities (money laundering, fraud, terrorist financing, sanctions evasion) may have the same impact on nationwide infrastructures, as a large scale cyberattack. The paper proposes the usage of blockchain technology for data collection and analysis, to serve as an early warning system for public and private organisations, in both cases – cyberattacks or associated illicit activities, like money laundering, crypto tumblers or black markets. Blockchain can be the core for an ecosystem of contributors for various cybersecurity services suppliers and sources, easing real-time detection, reporting, and alerts on high-risk activities.

Keywords: cyber-attack, blockchain, analysis, security, data, virtual assets, intelligence.

INTRODUCTION

Financial institutions are the targets of multiple cyber-attack types, with significant financial costs, but the effects may also include reputational damage or sanctions from regulators or supervisors. According to statistics from 2023, the average cost of a cyber-attack for financial institutions, was around 6 million USD and most of the attacks were focused on networking, applications (third-party) and account related (Petrosyan, 2023).

https://doi.org/10.54851/v5i2y202307

Phishing attacks in 2021 targeted mostly financial institutions and e-commerce entities, but also their customers as specific targets in malware campaigns. Cyber criminals are often financially motivated and are constantly finding more sophisticated ways to collect and move their illicit funds, this is why the financial dimension is crucial to address the fight against cybercrime.

In March 2023, the Financial Action Task Force (FATF), the international standard-setter on combating money laundering and terrorist financing, released its first report on ransomware. Ransomware is a type of malicious software involving data exfiltration, used by cybercriminals to deny access to data, systems, or networks, subject to a ransom payment.

The FATF report highlights that the payment and later laundering of ransomware funds is "almost exclusively conducted through virtual assets." It finds that Bitcoin accounts for 99% of payments, with Monero making up the rest (Financial Action Task Force, 2023). The ransomware market alone is estimated to reach some 265 billion USD by 2030 (Morgan, 2023).

Cyber criminals are also using an increasingly sophisticated set of virtual asset-specific technologies and techniques to launder and obfuscate the flow of their illicit funds and the solutions to address this challenge have to do with blockchain analytics. The traceability and immutability of the blockchain on which these virtual assets move offers unique opportunities to disrupt the flow of these ill-gotten gains.

Blockchain intelligence through analysis of publicly available information on the blockchains enables regulators, law enforcement and other industries to find and stop illicit entities. Public and private organisations could use the power of blockchain intelligence to fight cybercrime through public-private partnerships in the following three areas:

- Sharing information about risky or illicit activities through dedicated platforms;
- Building blockchain intelligence capabilities, as part of a broader suite of cyber intelligence and forensics capabilities;
- Partnering with experts to achieve prompt incident response.

CURRENT CHALLENGES AND OPPORTUNITIES

The current regulatory framework across the European Union (EU) requires all financial institutions to send a report on potential damaging cyber incidents in 24 hours, once found, according to the Network and Information Security Directive (NIS/NIS-2) equivalent, named Digital Operational Resilience Act (DORA). Article 33 of the General Data Protection Regulation (GDPR) also highlights that a report on a potential data breach should be sent within 72 hours to the competent authority.

Even if there are these obligations to send reports, there is high degree of not reporting or under-reporting the impact of a specific incident. Research from Bitdefender has shown that over 40% of IT professionals do not report cyber-incidents (Bitdefender, 2023). The reasons are due to fear of losing customers or risking fines or sanctions from regulators or supervisors.

In the case of the LinkedIn hack, the incident was officially announced only after the attackers have made public the list of passwords and usernames (Finkle Jim, Saba Jennifer, 2012). A similar case was the Target data breach, confirmed only after data was available on the dark web (Krebs, 2013).

In the case of financial institutions, the degree of under-reporting is difficult to assess, even if there is a regulatory framework in place to ease this process. The TIBER-EU regulation mandates the execution of regular exercises, based on specific collected threat-intelligence reports (European Central Bank, 2023). The need for such a regulation has risen due to a dissonance between tabletop exercises results and the real-world events, with cyber events occurring on a continuous basis.

In practical terms, any kind of cyber incident holds some significance for Open-Source Intelligence (OSINT) based data collection, which can be used in a pro-active way, to generate leads and prevent or disrupt other forms of attacks. This is why it was found the need to have a centralized responding entity to cyber incidents, materialized through the existence of Computer Emergency Response Team (CERT) units across the European Union. CERTs are obliged to cooperate because cyber-attacks on cross-border entities such as financial institutions, may affect not just the geographical location where an attack may have originated, but also some other geographical locations (EU CERT, 2023). The significant challenge for reporting cyber incidents to CERT units is linked to a specific type of data collection standard, commonly agreed and how data can be shared across multiple entities or domains.

A cyber-attack is not linear and can be executed with an exceptionally large degree of chaos and unpredictability. The non-linear characteristic is what makes the cyber-attack so effective. The definition of traceable elements like hostnames, IPs, services, are just means to try and give a somewhat linear character of a cyber-attack. This linearity allows tools like Firewalls to block incoming attacks. However, in the case of a denial-of-service executed at a business level, linear responses might not be able to block these types of attacks. Bad actors, especially in the case of state-level operations, have resources that are customised, and zero-days are usually employed primarily. This is where the blockchain can shine and offer a near real-time alert feed, so that institutions are not being affected substantially.

Institutions have a specific interest in data protection and anonymity for customers and their own operations, this is why the level of trust between all these entities may not be to the highest level to achieve prompt incident response. To overcome the trust challenge and ensure a standard of reporting allowing prompt incident response, deploying a data analysis platform would be an opportunity and a necessary step forward. Such a platform could make use of data provided in a privacy environment, with the benefits of real time alerts and information sharing, encouraging participation by financial institutions, other private organisations, and the public bodies.

PROPOSED TECHNICAL SOLUTION

The compliance obligations are forcing financial institutions to have significant investments in efforts to ensure data is effectively managed and secured, while also ensuring suspicious or illicit incidents are reported. On the other hand, public entities such as regulators, supervisors, law enforcement or prosecution authorities, need high quality data when fulfilling their duties. A national platform, with multiple data inputs and reporting capabilities, allowing incentives to ensure safe reporting, would allow for effective mitigation of cybersecurity attacks and risks related to money laundering, terrorist financing, sanctions evasions, fraud, or other irregularities.

The proposed solution highlights the opportunity of a holistic analysis approach, which would bring together recent innovations and improvements in secure data-sharing, while also using some native features of the blockchain technology:

- Privacy oriented: collecting data and ensuring the right access is given only to trusted parties to the functionality stack.
- Non-repudiation: the identity of the information provider is unique and unalterable.
- Cross-referencing data with input from commercial blockchain analytics providers.
- Automated Regulatory Implementation: the project supplies collector interfaces, as well as automated data agents to ensure that almost real-time data collection happens.
- Near-Real Time Alerts: any actor within the network is given an automated access to near real-time alerts per stored events in the blockchain.
- Socializing of the detection process: any entity interested in the participation can feed data in the blockchain using a specific interface. This offers the organisations from the private sector the ability to take part in the fight against illicit activities. There is also an important pool of available professionals, and the project can ease the access to these private resources.
- Democratization of the response to incidents: interoperability between public sector organisations could be significantly increased, using the default characteristics of a blockchain access (private contracts between chosen entities, supporting specific assignments and collaboration between specific stakeholders).

A combination of the following technology stacks can be the solution to the given issues:

- Blockchain: supports inherent zero-trust and transparency across the reporting and alerting chain.
- Encryption and privacy: using anonymizing functions and specific encryption methods for each data entity.
- Authentication: each incident is confirmed within the blockchain.
- Data streaming solution: the Application Programming Interfaces (APIs) endpoints must sustain millions of transactions per second, so a specialized queue is needed.
- A service mesh architecture with high availability and redundancy.
- Encryption in transit and at-rest.
- Analytics support.
- Extension APIs.
- Remote collection agents.
- Anonymizers.

The proposed technical solution can be seen in the below diagrammatic representation (Figure 1).

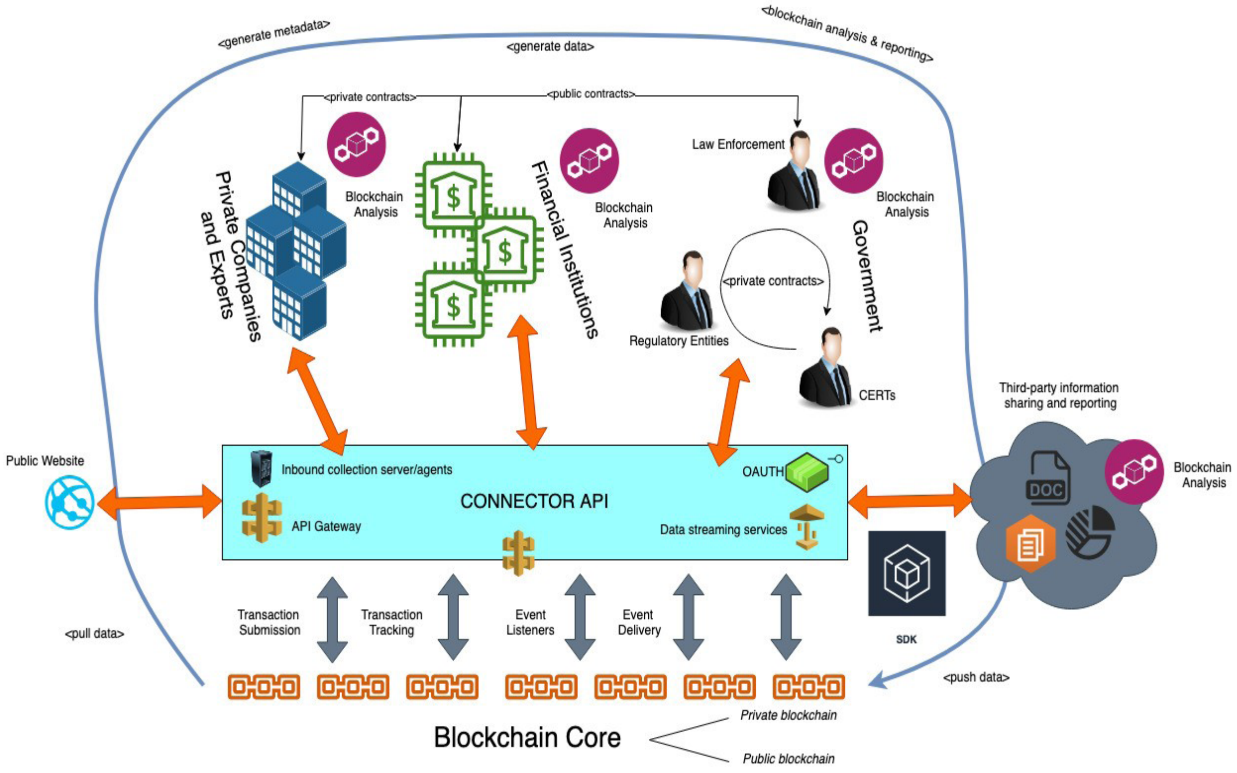

Figure 1. *High Level Architectural View*

The core architectural components are:

- Project's Managed Blockchain Platform:
  - Classified information sharing via the pluggable consensus and private contracts;
  - Standard information sharing within the network, as per the basic needs of this project;
  - Modularity and extension support;
  - Confidential information sharing via the selective consensus capabilities.
- Project APIs: the default access part to the blockchain for the information database. This choice in this case is to ensure that access to information is provided via a specific functional API.
- API Gateway: a standardized way to access the API, within the entire architecture of the system, will serve third-party actors interested in some way, in the provided data.
- Collector Servers: represent the first filter before any data is passed to the blockchain. The purpose is to separate the functional layer from the data input, with some form of cloud-based containers to be deployed. This is an optional part which could have multiple usage functions, including becoming a data bridge, allowing entities to supply specific data sets, and then using this part to map out the data to an internal standard.
- Data-matching across multiple data sets to find common risk indicators.
- Private sector entities: these could have access to a specific data set about indicators of cyber-attacks or other illicit activities, made available via a public service contract.
- Public sector entities: these can benefit from easing automated incident reporting, privacy, and security, together with a standardized data set to be collected and analysed.
- Financial sector entities: the core functionality will be covered by a local agent which can collect data in passive mode. This agent can be a simple web service, a reporting form, or an active device which sits on the edge of the security architecture.

The project would start by collecting several indicators, according to agreed reporting requirements, but the greatest feature of the proposed system is that it could be extended as needed, in terms of functionality.

The requirements to have up to date information about cyber incidents have evolved, as well as the methods deployed by potential attackers.

Examples of data sets to be collected are presented in Table 1, below:

Table 1. *Elements considered for reporting and analysis*

Data Collected	Reason
Origin IP	Used to create a list of originator IPs, to prevent further attacks at a geographical level. Also, can be used to create a list of malicious IP sources during an attack. The behaviour of some attackers during some attacks may leak their IPs, due to poor operational security.
Destination IP	The attacked target IP. This is particularly important, as it can show what the attacks may be after. In the case of financial institutions, the targets are usually specific.
Target Port	Is an indicator on the current attack campaign. Usually, the targeted port is also an indicator of what the attackers are after. If the targeted ports are HTTP(s) in nature, then a web attack is to follow (or a distributed-denial-of-service (DDoS)). Some malwares target specific ports.

Source Port	Is a definitive indicator of the type of malware used in some campaigns, as some malwares run on specific source ports for traffic.
Timestamp Detection	This is needed to create a basic timeline for the attack.
Timestamp Incident Start	This is needed to create a basic timeline for the attack.
Timestamp Incident End	This is needed to create a basic timeline for the attack.
URL	This is usually collected during web attacks.
Attack Vector	Estimated attack vector found by the response teams.
C2 List	List of Command and Control (C2) IPs, found by the response teams.
Suspected Filename Hashes	List of standardized hashes for the suspected files involved in an infection.
Phishing E-mail Content	The contents of the phishing email used on the attacks.
Phishing E-mail address	The email being the source of the phishing email attacks.
Phishing E-mail Headers	The headers of the phishing email.
Registry Modifications	In the case of some OS system registry modifications or system OS modifications, these will be supplied.
Alert Story	If any endpoint detection and response system (EDR) has issued any alert, the alert and detection rule should be supplied.
Common Vulnerability Enumeration Number (CVE ID)	If any response team can find some exploited CVE, this must be supplied.
Transactions involving virtual assets	Risky or illicit activities involving the use and transfer of virtual assets require the communication of details such as: wallet addresses, transaction hashes, IP addresses, DNS data, risk evaluations etc.
Domain Name System (DNS) Data	Any kind of resulting DNS data can help in assigning TTPs to attackers. This can be extracted from earlier supplied data.
Media Access Control (MAC) Addresses	If any MAC addresses are present in the packet frames, these should be supplied.
Hostnames	Any involved hostnames should be supplied. Notwithstanding hostnames cannot be supplied (usually) for attacking hosts, unless there are some other actions being taken, the targeted hostnames should be supplied.
Account names/Usernames	Associated impacted account names and usernames involved in the attack (if any).
Service/Service Version/Protocol	This is necessary to figure out the attack surface. This is a critical information that can help find incoming attacks, map out immediate measures and stop the attack before it happens.
Geolocation Data	If any kind of geodata is available, this should also be collected. This is especially useful when finding attack origins.
Traffic data	.pcap files holding traffic data.

The proposed technical solution can ease confidential data sharing, with the consensus system, which allows for bilateral information sharing, without any other entity in the network having access to that data.

Another important feature is to ensure that there is an auditable log data for each event if there is a requirement for tracing specific actions. The blockchain itself, could then be used as a basic data source for multiple data analytics tools. It could also be used as a generic national database for cyberattacks and other types of illicit activities, where multiple types of data could be stored.

The project will also support the development of commercial relationships between financial institutions and private service suppliers, using a dedicated market for required regulatory service suppliers. The choosing of a service supplier could be processed transparently, considering specific conditions, which can be covered by smart contracts issued on the blockchain.

Like haveibeenpwned (haveibeenpwned, 2023), which has become a source of verification for public entities, the proposed project has the potential to become a national database of cyber events, with highly advanced functionality for real-time response and alerts for private and public sector.

PROJECT TIMELINE

The project could be developed in phases, starting with a focus on cybersecurity and cyber incidents, each phase delivering some specific utility from the full set of functionalities. The core purpose is to allow data analysis by cross-referencing multiple data sets, with some metadata attached to them. However, the real value of the project would be its ability to be extended as needed, according to the risk assessments concerning national security and financial stability.

Using the blockchain as a source of authenticity, allowing input from multiple stakeholders with a focus on privacy and high-speed data sharing, can improve the local and regional responses to cyber incidents.

The expected development period for a Minimal Viable Product (MVP) is one year, as seen in the below Figure 2.

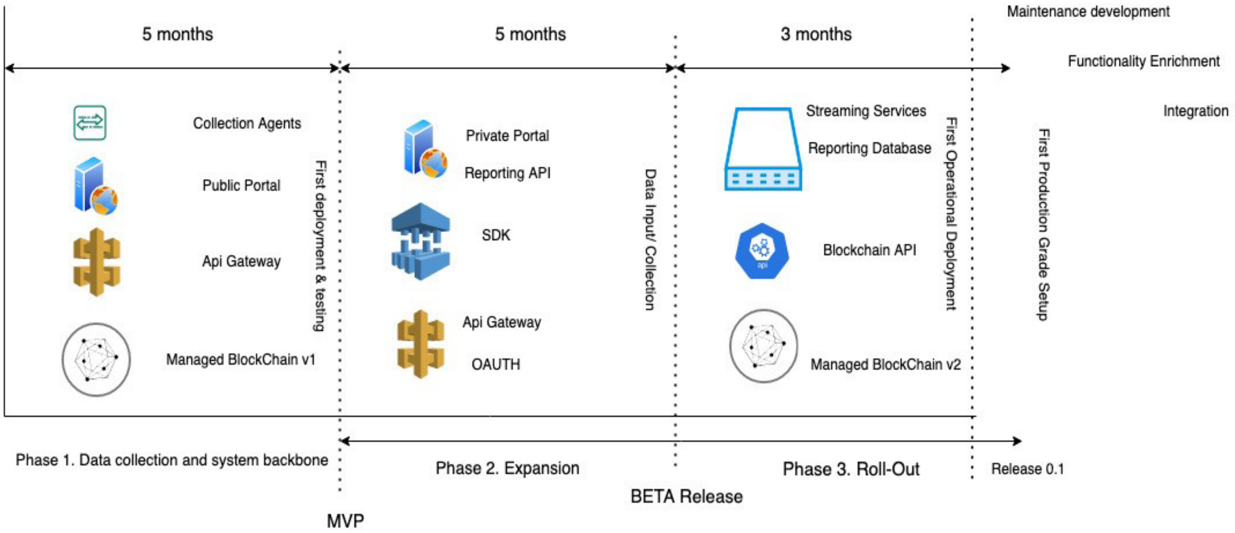

Figure 2. *Project Planning*

Phase 1. Data collection and system backbone.

The purpose of this phase is to setup the core functional elements of the project. The identified elements as core, are the blockchain, the API Gateway and the Open Authentication 2.0 Protocol (OAUTH) infrastructure, the public portal, and the collection agents. At this stage, data could be collected. The Minimal Viable Product (MVP) should be released when the components of this phase will be operational. It is envisaged that when the MVP will be released, some organisations could start taking part in the project, initiate profiles on the blockchain and supply data. Data collection and testing could be done using a community-based approach, where multiple types of entities can engage within the project to test out its core functionality for data collection, smart contract execution, alerts.

Phase 2. Project Expansion

At this step, more functionalities can be added to the public portal, a set of basic reports can be defined and supplied to the public. More advanced features can be added to split the collection and the processing levels of the application, by employing different staging environments for data, under the form of "Collector Servers." Within the architectural structure, this would be an optional part, given the blockchain implementation model chosen. One of the most important components of such a system is the Software Development Kit (SDK) and API sets, which must be delivered to allow for this project to be customizable and extended. The focus with this approach is to enable a community of experts that want to contribute, to deliver new functionalities and even help create a climate for new business and services development.

Phase 3. Roll-out

The final stage of the project is to create a No-SQL database with a streaming engine on top, for real-time alerts and other data mining purposes. Data stored in the blockchain could be structured in specific data structures, to be supplied on request, based on specific requirements. The purpose of this phase is to setup the interfaces and some basic data aggregates, as the database objects and structure can/will evolve over time.

VALIDATION BY USE CASE SIMULATION

Applying blockchain in cybersecurity defensive operations, as well as proactive operations, can result in multiple challenging cases.

In the case of a DDoS, employing such a system could instantly supply alerts across public and private sectors, stopping an attack right before it even starts, assuming entities that are struck by some random DDoS get to report it using the project's features and then any other entity that is a member within the network can proactively respond.

Security Operations Center (SOC) teams may have specific functionalities that allow them to take decisions faster, when analysing alerts, by allowing custom reporting and filtering, using basic criteria like:

- Time stamps;
- Source IP and Destination IP;
- Source Ports and Destination Ports;
- MAC Addresses;
- Hostnames;
- Account names/Usernames/Compromised Passwords;
- Emails;
- Protocols/Service Names/Service Versions;
- DNS Data;
- Geodata like country of origin;
- Virtual Assets Transactions (wallet IDs, transaction hashes, etc).

Making available .pcap files and allowing export for study purposes, can help SOC teams design and use new alerts in Security Information and Event Management (SIEM) products. Some basic functionalities like searching based on random strings and viewing aggregate data statistics, can again support defensive cyber operations and help develop alerts and proactive measures.

Public sector entities can actively engage in either blocking the attack and then doing threat hunting, or inform and add multiple mitigators, which can then be used by other network members. The private sector entities can engage in blocking any other attacks from running by activating denial-of-service mitigations before an attack can be executed.

Across the EU, due to the Ukraine-Russia conflict, the threat landscape has changed, and multiple threat actors have appeared with a declared scope of fighting within the conflict but are not necessarily militarized. Those are civilian units that act for the purpose of the state in various forms. One such group, called NoName, has shown capacity to strike within the EU territory and take out multiple targets using DDoS (Zoltan, 2023). However, the intel channels and evaluating their attacks on multiple targets, can be mitigated by blocking their specific methods. The role of the project in this case would be to limit the potential damage of such groups, preventing a widespread impact.

In the case of malware campaigns, these are static, however security researchers tend to find out the Indicators of Compromise (IoCs) and make them public on their own pages or websites. Having a system where they can be incentivized to upload these IoCs and data, can help both the security researchers and the network members.

BUILDING A BLOCKCHAIN INTELLIGENCE COLLECTION INFRASTRUCTURE

A recent report by FATF on ransomware highlighted the importance of such specialised capabilities, especially in the public sector (Financial Action Task Force, 2023):

„*Competent authorities should use and adapt, as necessary, traditional law enforcement techniques as well as virtual asset-specific techniques, to conduct ransomware-related money laundering investigations. Competent authorities should have the necessary specialised skills and expertise for successful financial investigations relating to ransomware. This includes development, access and training relating to blockchain analytics and monitoring tools.*" („FATF Report Countering Ransomware Financing")

Developing such capabilities can be eased by partnering specialist experts to achieve high quality data analytics, focusing on ability building on a national level. This would create the conditions to improve private-public partnerships, creating an opportunity to focus on how each stakeholder can maximize their contribution, while also benefiting from an integrated approach.

The paper calls out the importance of data analysis focused on strengthening reporting and monitoring abilities, public-private information sharing, including internationally. Disrupting illicit activities implies reporting and disclosure requirements, as well as prompt and relevant data sharing. A recent report, published in May 2023 by the European Systemic Risk Board (ESRB), highlighted the fact that there is limited information available to assess the exposures and impact of virtual assets, recommending that there should be a policy for monitoring, and standardised templates for regular reporting across competent authorities and financial institutions (European Systemic Risk Board 2023, 32).

Increasing ability and fostering a community of professionals would create the conditions to improve the amount and quality of data in a coordinated and consistent manner by implementing a national data analysis platform. Such a platform would allow better reporting, monitoring and information sharing in a privacy-controlled environment about emerging typologies, found red flags, enhancing awareness and knowledge on risks associated with virtual assets.

CONCLUSIONS

The use of cyber-attacks for financial or strategic goals has risen and it is not a new issue. The advancement of attack methods in the cyber domain, however, generates the need for a prompt response. The speed with which some attacks are executed can make them unstoppable or can have substantial (negative) impact. Blockchain is the best solution, to cover all the needs of an integrated nation-wide response infrastructure.

This infrastructure can supply a real-time data feed, coming from distributed and reliable institutions or private experts, to block malicious traffic, before it generates a real impact into a critical system.

The proposed blockchain system, with its open zero-trust approach, will ensure prompt incident reporting, alerting and damage control even in the case of Advanced Persistent Threats (APTs). All these features can be ensured, without the need to have access to confidential data, or endanger functionality of any contributor in the chain, with information leaks or cross-domain incidents. Each party will keep its function and ability to contribute to the chain.

The national data analysis platform will play a pivotal role in finding suspicious activity, watching risky transactions, and safeguarding national security and financial stability. The blockchain platform can therefore be used as a threat-intelligence feed for any security defensive mechanism. The proposed platform is essential in supporting the development of relevant abilities and create a community of professionals around it.

Thus, using blockchain analytics in the proposed infrastructure, will support the development of mechanisms or empower existing ones to respond to threats much faster than the existing status-quo.

REFERENCE LIST

Bitdefender. (5 April 2023) *The cybersecurity challenges businesses are facing in 2023 – Report*. https://www.bitdefender.com/blog/businessinsights/bitdefender-2023-cybersecurity-assessment/ [Accessed 14th July 2023].

Finkle, J. & Saba, J. (6 June 2012) *LinkedIn suffers data breach.* https://www.reuters.com/article/net-us-linkedin-breach-idUSBRE85511820120606 [Accessed 8th June 2023].

European Central Bank (ECB). (2023). *What is TIBER-EU?* https://www.ecb.europa.eu/paym/cyber-resilience/tiber-eu/html/index.en.html [Accessed 2nd April 2023].

European Systemic Risk Board (ESRB). (25 May 2023) *Crypto-assets and decentralised finance. Systemic implications and policy options*, https://www.esrb.europa.eu/pub/pdf/reports/esrb.cryptoassetsanddecentralisedfinance202305~9792140acd.en.pdf?853d899dcdf41541010cd3543aa42d37 [Accessed 28th May 2023].

European Union. (2023) *Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU)*. https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/computer-emergency-response-team-eu-institutions-bodies-and-agencies-cert-eu_en [Accessed 23 rd July 2023].

Financial Action Task Force. (14 March 2023) *FATF Report: Countering ransomware financing*. https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html

Financial Action Task Force. (2023) *The FATF focus on virtual assets*. https://www.fatf-gafi.org/en/publications/Virtualassets/Virtual-assets.html [Accessed 27th May 2023].

Financial Action Task Force (FATF). (5 July 20210) *Second 12-month review of revised FATF standards – Virtual assets and VASPs*. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Second-12-month-review-virtual-assets-vasps.html [Accessed 12th May 2023].

Hunt, Troy. https://haveibeenpwned.com [Accessed 19th July 2023].

Krebs, B. (23 December 2013) *Sources: Target Investigating Data Breach*. https://krebsonsecurity.com/2013/12/sources-target-investigating-data-breach/ [Accessed 18th May 2023].

Morgan, S. (7 July 2023) *Global Ransomware Damage Costs Predicted to Exceed $265 Billion By 2031*. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ [Accessed 12th July 2023].

Petrosyan, A. (2023) *Cybercrime and the financial industry in the United States - Statistics & Facts*. https://www.statista.com/topics/9918/cyber-crime-and-the-financial-industry-in-the-united-states/#topicOverview [Accessed 18th June 2023].

Zoltan, M. (29 March 2023) Liverpool City Council Website Targeted by NoName Hacker Group in Latest DDoS Attack. https://www.privacyaffairs.com/liverpool-city-council-ddos/ [Accessed 19th July 2023].