Blockchain Protects Our Data, But Who Protects the Blockchain?

OwlGaze
Cyber Security Software & Advisory

Table of Contents

Introduction 3

The Problem 3
- Lacking of Regulatory Intervention 4
- Social Engineering Attacks 4
- Supply Chain Compromise 4
- Ransomware Attacks 5
- DeFi Protocol Hacks 5
- Smart Contract Design Vulnerabilities 5
- Crypto Wallet Attacks 6

The New Approach 6
- Strategy & Governance, Risk, Compliance (GRC) 7
  - Cyber Strategy & Roadmap Development 7
  - Compliance & Regulatory Assessment 7
  - Educational Awareness Training 7
- Cloud & Infrastructure Security 7
  - Cloud Security Management 7
  - Secure System Development Lifecycle (SSDLC) 7
  - Vulnerability & Patch Management 7
- Identity & Access Management (IAM) 8
- Data Privacy & Protection 8
- Managed Detection & Response 8
  - 24/7 Threat Monitoring - Security Operation Center (SOC) 8
  - Incident Response Playbooks 8
- Predictive AI Software 9
  - AI Fuelled Event Correlation 9
  - Combined Compliance & Security 9
  - Native Cyber Threat Intelligence Enrichment 9
  - Machine Learning (ML) Based Alert Fine-Tuning 9
  - Resilient Architecture 9

Benefits and Proof Points 10
- Ubiquitous Cyber Maturity 10
- Advanced Technical Expertise 10
- Greater Visibility 10
- Predictive Capabilities 10

Critical Success Elements 11
- Advanced Technologies 11
- Optimal Resource Allocation 11
- Positive Cyber Culture 11
- Best Practice Mindset 11

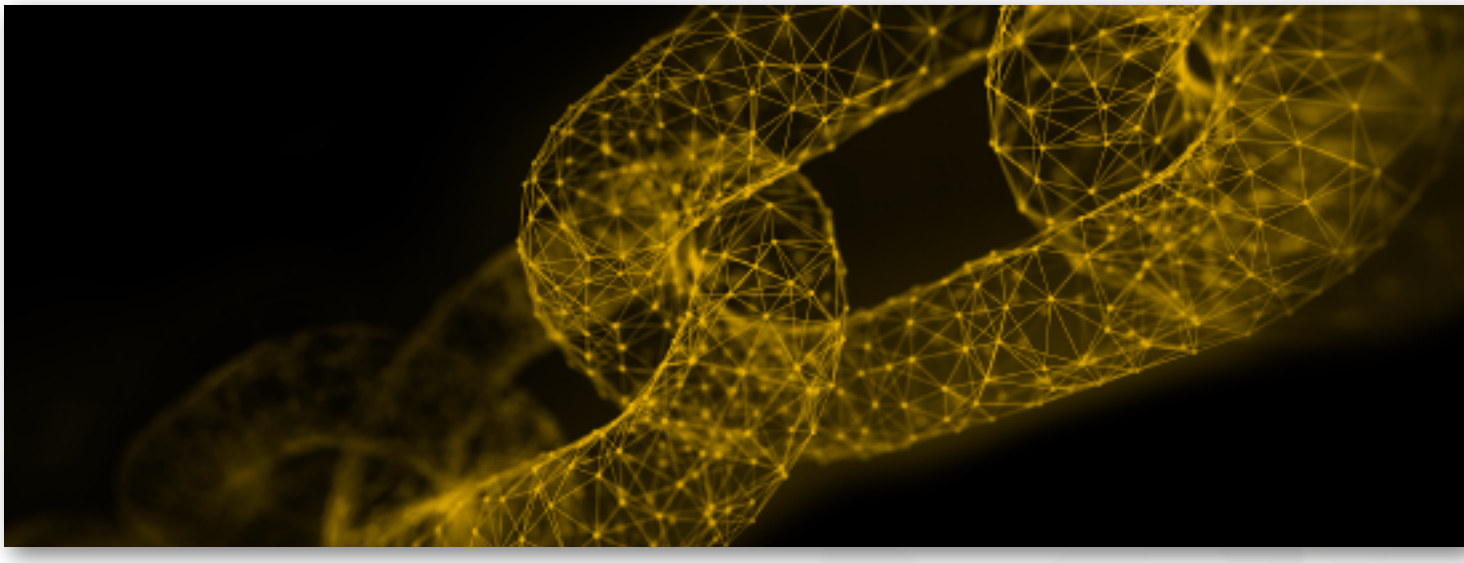
Closing Remarks 12

Introduction

The global financial crisis of 2008-09 resulted in the development of the Bitcoin whitepaper which introduced the world to the idea of blockchain technology and cryptocurrency. Within blockchain, information is stored in several databases (blocks) that are linked together chronologically through cryptographic hashes to form a distributed network (chain). Since its inception, several organisations are leveraging blockchain in areas where maintaining data integrity is the need of the hour. With the entry of Ethereum, solidity-based application development and smart contract architecture, it has created a burst of new ventures with innovative products. New use-cases are proliferating across trade, banking, financial services & insurance (BFSI), healthcare, media, F&B, and philanthropy, to name a few. The global blockchain market is expected to hit USD 67.5 billion by 2026. Within the realm of BFSI, the evolution of cryptocurrencies as an asset class for investors has furthered the commercialization of blockchain technology through decentralised finance (DeFi) services. As of 2021, there are over 6,000 cryptocurrencies being traded freely with global cryptocurrency market capitalise reaching USD 990 billion. Serving investors' needs are exchanges, lenders, asset managers, custodians, cross-border payment applications, and clearing & settlement houses that all benefit from the surge in blockchain use-cases.

Despite the increasing penetration of blockchain and the astronomical valuations of related businesses, a lack of global regulations, standards and guidelines has put all players in a grey area. Moreover, the technology is still in its nascent stages where several design and development vulnerabilities place blockchain architecture at a higher risk of exploitation by bad actors. This security problem further extends to companies exclusively storing and/or transacting cryptocurrencies through digital wallets.

This paper aims to highlight the prominent security challenges faced by companies operating or dependent on blockchain systems. It further suggests an organised approach towards tackling both regulatory and cybersecurity challenges as a joint effort.

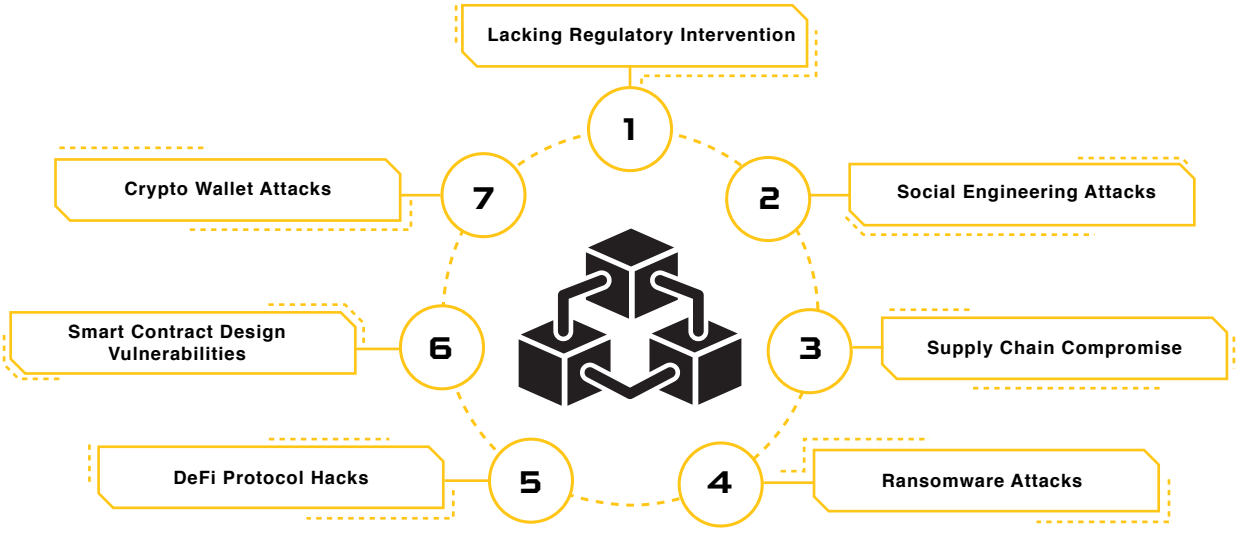


The Problem

Blockchain gained traction from its ability to provide data immutability, meaning that data stored within the blocks cannot be changed or tampered with. This benefit stems from the comprehensive chronological inputs used in the hash computation mechanism. However, if blockchain is protecting the data, who is protecting the blockchain?

There are several known vulnerabilities and attacks facing the blockchain architecture that were discovered since its early days including 51% attacks, time jacking, crypto jacking, forking attacks, eclipse attacks and smart contract vulnerabilities such as re-entrancy attacks, overflow attacks, and balance attacks, to name a few.

Key Cyber Challenges For Blockchain Companies



That said, challenges faced by blockchain companies exceed the infrastructure and can adversely impact multiple components of the organisation. Some of those key challenges are:

1 Lacking of Regulatory Intervention:

In 2019, much after the Bitcoin price surge and subsequent crash, the SEC released The Investment Contract Framework, TurnKey Letter & PoQ Letter, which jointly classified digital assets as viable or non-viable investment contracts. Prior to that, there was no official documentation to draw such conclusions. With a rise of innovative business models leveraging blockchain technology, several billion-dollar organisations find themselves operating in a grey area resulting from an absent regulatory intervention. This is particularly true for organisations disrupting traditional industries by amalgamating legacy systems with blockchain Infrastructure.

2 Social Engineering Attacks:

Adversaries are attacking organisations at their weakest link, the users. Users include employees, customers, shareholders, and other stakeholders who have access to the enterprise environment. Adversaries often steal credentials to gain access to user accounts and then try to escalate privileges to steal data or tokens. When users are not trained properly, they often fall prey to phishing or other forms of impersonation attacks. Users that hold private keys to crypto wallets or a privileged status are at a higher risk of getting targeted.

3 Supply Chain Compromise:

Digital transformation is paving the way for new and innovative technologies that increase the overall productivity of the business through streamlining and standardisation of processes. This has largely led to an increase in multi-vendor environments which are all connected to the enterprise network. Adversaries can exploit age-old legacy systems and gain access to mission critical blockchain facilities storing or processing digital asset transaction traffic. With a large-scale migration to the cloud, this threat has never been more relevant for all organisations.

4 Ransomware Attacks:

Financially motivated adversaries can gain access to enterprise environments and encrypt proprietary files, rendering them unreadable. Companies are forced to pay a ransom in exchange for decrypting their files. Despite the lack of guidelines, blockchain and crypto companies are still required to abide by data privacy and protection regulations. Ransomware attacks can hamper data availability and result in long-drawn downtimes until data is available for business operations. The onset of remote working and lack of cyber awareness have paved the way for favourable conditions to launch ransomware attacks. Since cryptocurrencies are also used as an agent for ransom extortions, organisations in the blockchain space with reactive cyber maturity level are soft targets for bad actors.

5 DeFi Protocol Hacks:

Simply put, decentralised finance (DeFi) organisations perform all the traditional BFSI activities over a blockchain system where a single centralised authority does not govern them. If left unsecured, adversaries can gain access to networks and self-authorise transfer of digital assets to their own addresses.In 2021, approximately USD 12 billion invested in DeFi protocols was lost to scam and theft, out of which about USD 2 billion was lost to malicious attack campaigns. That year also witnessed the single largest DeFi cryptocurrency hijack of USD 600 million. With nearly USD 240 billion locked in, DeFi protocols are a certain target for adversaries.

In 2021, approximately USD 12 billion invested in DeFi protocols was lost to scam and theft, out of which about USD 2 billion was lost to malicious attack campaigns. That year also witnessed the single largest DeFi cryptocurrency hijack of USD 600 million. With close to USD 240 billion locked in, DeFi protocols are a certain target for adversaries.

6 Smart Contract Design Vulnerabilities:

Smart contracts allow seamless automated transactions by introducing inter-party trust in deals through an escrow mechanism. Under the DeFi umbrella, smart contracts are largely used in interoperability protocols which link multiple blockchains together. Design flaws can allow adversaries to call privileged smart contracts controlling the flow of digital information between linked blockchains. The assets can then be directed into an adversary-controlled address to be traded freely over an exchange. Organisations leveraging the smart contract technology need a secure system development life cycle through DevSecOps considerations.

7 Crypto Wallet Attacks:

Like wallets used to store cash, cryptocurrency is deposited in digital wallets which can be accessed through cryptographic keys. There are two sets of keys, first the public key, which can be used to deposit digital assets in an address just like a bank account number, and secondly, a private key, which can be used to withdraw money from the wallet like a pin number. Private key security is critical to safeguarding the digital assets stored within crypto wallets. Basic attacks on crypto wallets aim to locate files where private keys are stored. However, since 2018, attackers are re-constructing private keys by decoding electromagnetic signals emitted by devices in an attempt known as side-channelling attack. Additionally, several attacks on crypto wallets leverage human error, pre-existing vulnerabilities and connection interception which eliminates the need for private keys to hijack a wallet.

Rising complexity of attack tactics, techniques & procedures (TTPs) coupled with uncertainty about regulatory intervention have put blockchain and crypto organisations at an urgent need for proactive cyber threat management.

> **Since 2018, attackers are re-constructing private keys by decoding electromagnetic signals emitted by devices in an attempt known as side-channeling attack.**

The New Approach

Every comprehensive cybersecurity program starts from fundamentals of basic cyber hygiene working its way up to advanced controls. Since every organisation operates differently, a one-solution-fits-all approach doesn't work. At OwlGaze, we carefully study the enterprise environment and its crown jewels to curate a tailor-made roadmap leading towards greater cyber resiliency.

Protecting the blockchain infrastructure and organisational components such as devices, users, and data stored on blockchain, or not, all necessary to achieve a higher cyber maturity. These threats can surely be tackled separately but should be guided by the same overall strategy. OwlGaze brings the best of security advisory and software to help blockchain leaders innovate without the fear of hackers or regulatory upheavals, and recommends the following core focus areas:

1 Strategy & Governance, Risk, Compliance (GRC):

Cyber strategy plan joint with established policies and supporting GRC processes form the skeleton of security controls, a must-have for all blockchain companies. It provides direction to the program and helps management allocate an optimal budget to the cybersecurity department. Initiatives that support this include:

Cyber Strategy & Roadmap Development:
A cyber strategy supported by a comprehensive assessment will help identify and mitigate the threats and strengthen the overall cyber security posture with the ever-evolving cyber threats landscape impacting the blockchain industry, enabling you to build a short-term and long-term cyber roadmap. Aligning controls against industry standard frameworks, such as NIST, ISO and SOC2, to identify internal security gaps and supply chain risks allows a prioritised approach on building a secure scalable eco-system.

Compliance & Regulatory Assessment:
Organisations are still trying to understand how the structure and complexity of blockchain fits into the evolving privacy, compliance, and regulatory environment, such as GDPR and similar law. Performing a detailed review of organisational controls with regards to the regulatory requirements to ensure compliance within the desired timeframe allows a proactive approach to complying with the requirements.

Educational Awareness Training:
All stakeholders, including end-users (clients), need to be aware of prominent cyber threats and the financial or operational consequences of their actions. An organisation's security can be easily impacted by an employee or human error. OwlGaze specialises in conducting frequent trainings, wargaming workshops targeting different security levels and business environments can lead to a proactive approach of recognizing, reporting, or eliminating a potential security threat.

2 Cloud & Infrastructure Security:

Technological infrastructure utilised by business users need to be secured to minimise the attack surface needs. As businesses migrate to the cloud, managing the attack surface has become more complicated. Establishing and continuously enhancing the following capabilities are essential:

Cloud Security Management:
Cloud security is constantly evolving, but a handful of best practices have remained constant for ensuring the security of cloud environments which includes at minimum understanding your shared responsibility model, leveraging a Cloud Access Security Broker (CASB), intrusion detection and prevention technology and enforcing cloud security policies. For blockchain, scalability is the antithesis of decentralisation because it has constrained computation and storage capabilities.

Secure System Development Lifecycle (SSDLC):
Most blockchain systems are plagued with design flaws and bugs during the product development phase. Software development teams need to align and collaborate with security teams to instil security by design principal. DevSecOps processes and tools to identify security flaws at an early stage allow blockchain architects and developers benefit from employing CI/CD practises for timely and secure product releases.

Vulnerability & Patch Management:
Despite continuous source-code testing during initial system development, a company’s environment can be attacked through vulnerabilities from other software and tools integrated from third-party service providers. For blockchain based developers, it may also involve integrations with other blockchains containing vulnerabilities or improperly designed interoperability protocols, limiting scalability. Proactively indentifying vulnerabilities across connected systems, can avoid platofrm milconfiguration, communication uncertainty, errors in application development specifications, and cross-chain logic issues.

3 Identity & Access Management (IAM):

Most digital asset storage wallet hacks were carried out after the adversary gained access to valid user accounts and consequently evaded security defences. Such attacks could only be detected at a post-compromise phase after the assets have been stolen from user wallets. To detect suspicious behaviour earlier in the attack chain, organisations need to proactively monitor user account activity. Defining and developing an end-to-end IAM strategy based on the principle of least privilege is fundamental. Continuous monitoring from on-boarding to off-boarding employee to privileged admin users, identity governance and administration (IGA) is a foundational security control.

4 Data Privacy & Protection:

Data protection is imperative for all organisations alike. Sending or storing sensitive data using cryptographic algorithms is not enough to protect against man-in-the-middle attacks. Blockchain companies need to further decide between storing data on-chain and off-chain. Securing data in-transit between on-chain and off-chain systems also needs to be considered. Applying the principle of Confidentiality Availability and Integrity (CIA) to your data is the step forward towards understanding how to protect your sensitive and mission critical data resides. Combined with aligning to privacy and regulatory requirements that are applicable to the industry and across different jurisdictions (GDPR, CCPA, PDPO etc.) will provide a holistic view of your data landscape.

5 Managed Detection & Response:

Deployment of preventive controls doesn't guarantee full protection against bad actors. As adversaries get creative with their attack techniques, blockchain based organisations must be prepared to detect and handle cyber-attacks real-time. Up-scaling within the following key areas is a step forward:

- **24/7 Threat Monitoring - Security Operation Center (SOC):**
  Continuous security monitoring and real-time threat prevention is key to stopping unauthorised activities at an early stage, lowring the impact of operational impact intensity when the enterprise environment is compromised and therefore reducing the potential financial impact.

- **Incident Response Playbooks:**
  Readiness is key in an attack scenario it is crucial to save time before an adversary establishes control over the critical infrastructure. Develop and define tailor-made incident response playbooks which include step-by-step processes to contain, eradicate and recover from unauthorised activities. Playbook workflows are periodically updated, simulated and in-house staff is trained to optimise the response and recovery process.

6 Predictive AI Software:

Past attacks faced by digital asset firms have often been reported only after an illicit transaction was successfully executed on or across blockchain(s). Detection of cyberattacks later in their lifecycle can lead to adverse financial, reputational and/or regulatory impact. To address this gap, the team of cyber experts at OwlGaze developed Blacklight, an AI powered predictive next-generation cyber software with the following key functionalities:

AI Fuelled Event Correlation:
Blacklight's advanced correlation engine combines the power of statistical modelling, supervised and unsupervised learning with rule based cyber threat analysis for accurate prediction of security threats. Blockchain and crypto firms can deploy Blacklight to correlate suspicious on-chain and off-chain activities for enhanced visibility of their security posture, simplifying both threat detection and incident response activities.

Combined Compliance & Security:
Blacklight is built with native out-of-the-box compliance alerting and advanced analytics to identify and flag compliance breaches. In an uncertain regulatory environment, Blacklight enables blockchain and crypto firms to monitor compliance and cybersecurity events under the same joint effort.

Native Cyber Threat Intelligence Enrichment:
Interoperability protocols, digital asset storage facilities, wallet addresses, and keys are important components for the blockchain and crypto industry. Identification of cyber risks affecting blockchain specific infrastructure is key to the development of proactive cyber maturity efforts. Blacklight's contextualised native intelligence monitoring, enriches the threat detection rules with near real-time industry specific intelligence feeds to identify bad actors and APT group campaigns.

Machine Learning (ML) Based Alert Fine-Tuning:
False-positive alerting generates tremendous noise for security teams globally. Blacklight's machine learning engine observes historic true and false positives for similar events using enforced learning to decide whether an alert should be triggered.

Resilient Architecture:
As blockchain and crypto firms undergo rapid expansion, they require technologies that can match their ambitious plans. Blacklight is both horizontally and vertically scalable. The deployment architecture can simultaneously span across on-premise data centres and multiple cloud service providers.

A cybersecurity program covering all the above areas will provide comprehensive coverage against security and regulatory risks. OwlGaze specialises in next generation predictive AI-based software along with an end-to-end cyber advisory leaving no stone unturned, driving an organisation on a path towards greater cyber resiliency.

Benefits and Proof Points

There are ample benefits which come from following a holistic approach for security blockchain infrastructure aligned to industry best practices. Some notable benefits are:

1 Ubiquitous Cyber Maturity:

Complex technological infrastructure results in the need for holistic cyber maturity across all assets, users, applications, data, and networks. A comprehensive cyber program will minimise the organisational attack surface and pave the way for fearless innovation across all business units.

2 Advanced Technical Expertise:

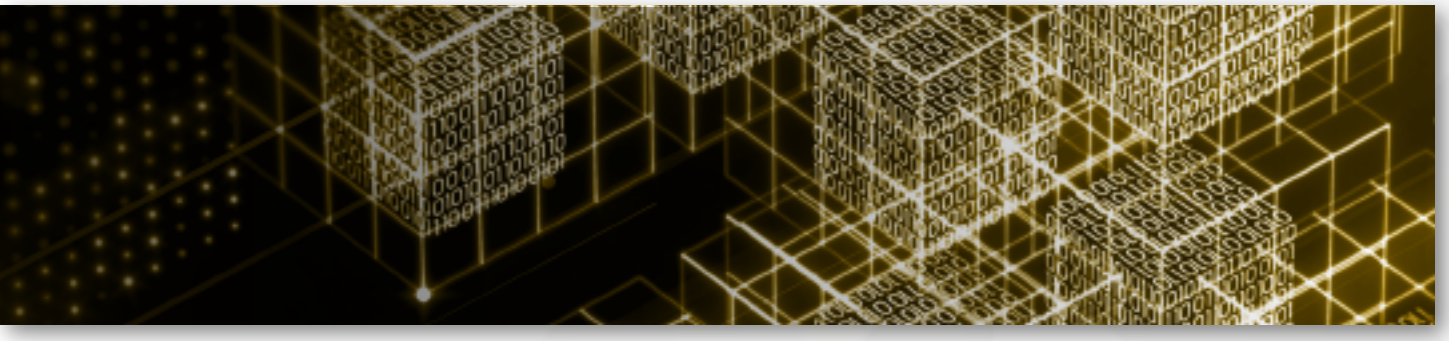
Businesses often struggle to properly enforce and execute the recommendations received from advisory firms. Besides providing actionable insights, the implementation and operations is key. Strategic security partners can be an extension to your team and provide additional industry insight.

3 Greater Visibility:

As organisations grow, dependencies across different functions and processes increase. To make informed decisions, management requires full visibility on all processes and factors impacting cybersecurity and not view them in silos. We help provide businesses with a holistic program covering all areas of cybersecurity under a single umbrella to prevent myopic decision making.

4 Predictive Capabilities:

To ramp up their defences against threat actors and fraud, blockchain and crypto firms need to aim for higher cyber maturity levels focused on stopping the adversary before they can impact the business continuity of the enterprise. As a predictive SOCaaS, Blacklight enables security teams to identify attack campaigns early, thereby fortifying the critical blockchain infrastructure.



Critical Success Elements

Cybersecurity is a continuous function that needs to adapt to an organisation's changing threat landscape. Blockchain companies should use rising cyber threats in the industry as a cue to develop a comprehensive cyber programs while considering several factors:

1

Optimal Resource Allocation:

A dedicated team of cybersecurity professionals must ensure that the organisation is always protected from inevitable cyber threats. Management needs to conduct regular feasibility studies and allocate budget to enforce cyber controls across the enterprise environment.

2

Positive Cyber Culture:

Employees, customers, and 3rd party stakeholders should be encouraged to proactively report suspicious activities on their devices or accounts. Establishing and promoting a security culture will improve inter-party trust and help to recognize attack campaigns earlier.

3

Best Practice Mindset:

Aligning best practices, proven methodologies and industry standards enable stakeholders to make inform decisions and solve problems. As organisations grow, dependencies across different functions and processes increase. Security leaders require full visibility on all aspects of the digital eco-system.

While senior management and cyber leaders are accountable for their company's cybersecurity, they are not the only ones responsible. All internal stakeholders need to be reminded regularly of the impact their job can have on the organisation's digital security. Onboarding all stakeholders to this cause will promote a vigilant mindset benefiting the organisation optimally.

Closing Remarks

Navigating a challenging environment and adopting the best practices can be overwhelming for business and function leaders. With the intertwining of blockchain and cybersecurity in an ever-evolving threats landscape, it is imperative that you continuously enhance your business to match the current landscape. Without proper thought, this implementation can be difficult or even impossible. Blockchain offers many benefits, such as efficiency, optimisation, cost reduction and better security. However, technology also introduces new risks to systems if not properly managed and monitored.

OwlGaze's Blacklight software provides an all-in-one scalable approach that can empower businesses to continue their growth and innovation objectives without fearing cyber threats. Blacklight combines a holistic approach of using predictive insights to reduce response times with a managed approach to take increased responsibility and accountability when it comes to your cybersecurity.

Blacklight – Built to secure your blockchain.

A revolutionary predictive threat detection solution to identify, prioritise and prevent cyber attacks using advanced correlation and AI. Helping you navigate your way through the disjointed layers of security providing a robust solution for real time security detection and monitoring. The first-ever truly predictive, cloud-native, AI-powered detection software that acts as a command center for any organisation.

Get in touch with our team of seasoned cyber security professionals and protect your business from evolving cyber threats today:

Ralph Chammah

Chief Executive Officer
ralph@owlgaze.com

Miro Pihkanen

Chief Security Officer
miro@owlgaze.com

About Blacklight & OwlGaze

Predictive AI-based threat detection & near real-time monitoring software. Enabling a proactive approach to identify, prioritize and prevent cyber attacks using advanced correlation and AI. Accelerated detection and decision-making. OwlGaze is a software and advisory company with a world-class team of cybersecurity experts, enterprise software developers and AI engineers. OwlGaze offers end-to-end cyber security services with deep technical expertise across all pillars of cyber and provide the next-in-class cybersecurity software.

OwlGaze
Cyber Security Software & Advisory

UK & EMEA

+020 3795 0401

info@owlgaze.com

2 Floor, Berkely Square House,
Berkeley Square, W1J 6BD
London

Asia Pacific

+852 3611 0130

info@owlgaze.com

36 Floor, 41 Heung Yip Road,
Wong Chuk Hang
Hong Kong

owlgaze.com @OwlGaze @owlgazecyber