AMBER | thoughtworks

Digital Asset Security, Compliance and Risk Management

White Paper

JOINT PUBLISHING

AMBER

thoughtworks

CONTRIBUTORS

SLOWMIST

BLOCKSEC

RIGSEC

ANCHAIN.AI

ankura

TABLE OF CONTENT

RECOMMENDATION I - AMBER GROUP

Swept by the wave of digitization, governments and enterprises worldwide are actively embracing the era of a booming digital economy. As an essential engine of economic growth and a new way of transferring value, digital assets are leading human society to embark on a brand-new journey of technological exploration. In the wave of the digital economy, digital assets represented by blockchain technology continue to drive the tide of technological innovation and business change. Cryptocurrencies, digital securities, digital artworks and other digital assets are changing the economic landscape at an unprecedented pace, thus becoming the new driving force of the digital economy.

At the same time, the digital asset industry is facing some challenges. The complexity and uncertainty of market competition, policies and regulations, and technological change pose various business risks for companies and investors. Governments worldwide are also developing regulatory frameworks to ensure a clear and rational future development of the industry. During its booming beginnings, many raised concerns about the security of digital assets. Revolutionary changes in smart contract technology, particularly the rise of platforms such as Ethereum, have brought great opportunities to the blockchain ecosystem as well as new security challenges. Hacking attacks due to smart contract vulnerabilities have exposed digital assets to significant security threats.

Amber Group is committed to building a more secure and reliable digital asset ecosystem. For this reason, we joined forces with technology change pioneers such as Thoughtworks, SlowMist, BlockSec, RigSec, AnChain.AI and Ankura, Web3 security gurus, and digital asset compliance consultants to discuss the latest advances and future trends in blockchain security. This whitepaper is the result of our discussions.

We hope to contribute to the safe and stable development of the digital asset industry and lead it to a safer, fairer, and more accessible digital future.

Thomas Zhu, Chief Technology Officer, Amber Group

AMBER

RECOMMENDATION II - AMBER GROUP

In recent years, continuous tech developments, recurring hacking attacks, and frequent regulatory changes in the Web3 and digital asset industries have demanded greater efforts from digital asset management institutions to adjust.

In order to effectively respond to these challenges, institutions need to establish frameworks and mechanisms for quality security management, compliance management, internal control management, and risk management.

Since its inception, Amber Group has strenuously invested in security, compliance, internal control, and risk control to strengthen the foundation of enterprise security and risk governance. This has allowed us to create a solid yet flexible set of risk control mechanisms to ensure financial and information security and upkeep compliance requirements.

Amber Group has joined hands with leaders from various fields in the industry to compile the white paper on "Digital Asset Security, Compliance, and Risk Management". The paper covers crucial topics relevant to digital asset management institutions, including organizations in security management, compliance management, internal control management, and risk management.

The whitepaper is the result of our efforts to provide practical guidance for digital asset management organisations to strengthen risk control, improve compliance measures, and ensure asset security. It offers an in-depth yet accessible analysis – including case studies – of the industry's technical aspects, compliance requirements, and regulatory standards. We hope it can help institutions deal with an increasingly challenging context.

The whitepaper was made possible thanks to our competent partners. We pledge to continuously drive innovation and promote synergy between industry leaders to accomplish greater achievements.

Leo Que, Chief Information Security Officer, Amber Group

AMBER

RECOMMENDATION III - THOUGHTWORKS

With the rapid development of blockchain and digital assets, security, compliance and risk control have become the industry's top priority. This whitepaper systematically combines through the risk and security challenges faced by the digital asset field, such as the complexity and variability of the blockchain, the risk of fraud and malpractice, hacker attacks, the evolution of the regulatory environment, etc. And shares the industry's best practices of the leading companies in the Web3 security system, transaction security technology, cyber-threat defense, and the construction of the compliance system. It is worth mentioning that the whitepaper also puts forward the concept of BizDevSecOps deep defence, and AISec smart contract vulnerability detection technology, showing the forward-looking thinking and technical perspective of digital asset security construction.

As a pioneer in digital transformation, Thoughtworks has rich experience in blockchain and fintech projects. We believe that deepening security, compliance and risk control is the key to the sustainable and healthy development of the digital asset ecosystem. We are willing to work with our industry partners to help enterprises build their security capabilities and jointly promote the standardized development of digital asset security through digital security built-in, DevSecOps process improvement, and automated security testing solutions. We welcome industrial interactions, open source initiatives, and the sharing of ideas to advance the development of this industry.

Ran Xiao, VP of BFSI China, Thoughtworks

RECOMMENDATION IV - THOUGHTWORKS

As a global software and consulting company, Thoughtworks has a unique culture of technical excellence, and in 2017 a few of our colleagues, with a great passion for new technologies, assembled a team to provide blockchain services to a number of large and medium-sized companies. Along the way, we have sensed that the shift from Web 2.0 to Web3 is a paradigm shift. It has changed the way we define data and interact with digital assets. Decentralization through blockchain and distributed ledger technology empowers individuals with unprecedented control over their data and transactions. However, this newly gained autonomy comes with a host of security challenges. The inherent transparency of blockchain technology, while increasing the accountability of the "strongest to be transparent," also exposes vulnerabilities that can be exploited by malicious actors. Smart contract vulnerabilities, insecurity of decentralized applications (dApps), and the evolving threat landscape require a comprehensive approach to digital asset security.

We believe that the complex interdependencies of business design, security development, security operations, and overall operations in the Web3 environment similarly require the emergence of BizDevSecOps-a complete process of security built into business development operations, and that these practices, which are already built into all aspects of FinTech-type businesses. These practices, which have been built into every aspect of the FinTech business, are also applicable to the product development process of Web3, the most prominent feature of which is one word - fast. Because the underlying blockchain platform is almost completely transparent to transaction data, automated engagement is much more efficient. In the face of exponentially growing transaction and contract volumes, it becomes more operational to leverage the power of AI for proactive threat detection, risk mitigation, and compliance detection. We have observed that AISec can better address the security challenges of digital assets in terms of anomaly detection, threat intelligence, intelligent security analytics, and automated security response.

Thoughtworks understands that the Web3 world is vast and limitless, which is why we have joined forces with a number of industry pioneers, including the Amber Group, to write this whitepaper. We hope that the knowledge and strategies in this whitepaper will continue to be iterated and upgraded in the industry, safeguarding the security and compliance of digital assets, and building power to preserve the transformative potential of Web3.

Shangqi Liu, Head of Hong Kong and Macau Market, Thoughtworks

RECOMMENDATION V - SLOWMIST

With the rapid advancement of technology and the wave of digitization sweeping across the globe, governments and enterprises around the world are actively engaged in the booming development of the digital economy. In this unprecedented era, digital assets, as an important engine of economic growth and a new way of value transmission, are leading human society to embark on a brand-new technological exploration journey. In the wave of digital economy, blockchain technology, as a representative of digital assets, continues to lead the trend of technological innovation and business change.

Digital assets have experienced a journey from savage growth to moderate regulation, and digital assets represented by blockchain technology are becoming a key engine of growth in today's economy. In the digital economy, digital assets with blockchain technology as the underlying layer, such as cryptocurrencies, digital securities, digital artworks, etc., are changing the economic landscape at an unprecedented speed and becoming the new driving force of the digital economy.

However, the booming development of digital assets is also accompanied by new challenges and risks. Business risks in the digital asset industry, including challenges in market competition, policies and regulations, and technological changes, have brought complexity and uncertainty to companies and investors. At the same time, digital asset regulation is facing a tortuous and volatile process. Governments around the globe are busy drafting regulatory frameworks for digital assets, and a clear and reasonable regulatory framework is considered key to the future development of the digital asset market.

In the wave of development of digital assets, the rise of blockchain technology has triggered a great deal of concern about the security of digital assets. Smart contract technology such as Ethereum has revolutionized the blockchain ecosystem, but it also faces security challenges. Hacking attacks due to vulnerabilities in smart contracts have caused huge losses to the entire blockchain industry, exposing assets to great security threats.

In this context, we bring together Amber Group's rich experience in digital asset management and SlowMist's rich experience in security to discuss the latest progress and future trends in blockchain security from the direction of compliance, Audit, MistTrack, etc., and commit to building a more secure and reliable digital asset ecosystem. Let's work together to create a digital future and contribute to the long-term and stable development of digital assets.

Zhang Lianfeng, Chief Information Security Officer, SlowMist

RECOMMENDATION VI - BLOCKSEC

As security practitioners dedicated to building Web3 security infrastructure, we are well aware of the risks and challenges faced by Web3 project parties on a daily basis. Years of security practices have shown us that we are in dire need of an action guide that has both a macro perspective and practical relevance to help us establish comprehensive security management, compliance management, internal control management and risk management frameworks and mechanisms to effectively address these challenges. This is precisely the significance of this white paper.

This whitepaper, led by Amber Group and co-authored with technology innovators, Web3 security leaders and digital asset leaders, brings together the experience and knowledge of all parties. We were fortunate to be able to participate, contributing our expertise and in-depth analysis. In the process of writing this paper, we focused on the monitoring part of the Web3 project's operational process and shared our practical experience in building and utilizing Phalcon Block to implement attack blocking to protect on-chain assets, hoping to provide readers with comprehensive and in-depth insights that will benefit more industry participants.

We expect this whitepaper to inject new vitality into the security, compliance and risk management of the digital asset industry, promote the safe, stable and prosperous development of the industry, and contribute to building a safer, fairer and more open digital future.

On the way forward, let's work together to build a safe, fair and open Web3 world.

Wu Lei, Co-founder, BlockSec

RECOMMENDATION VII - RIGSEC

The wave of digitization has become a new driving force for the economic development of countries around the world. Blockchain is one of the emerging information technologies of the digital economy, breeding new business models and industrial patterns, and is an indispensable cornerstone of the digital economy ecosystem.

Compared with the traditional Internet, Web3 faces many new security issues and threats; at the same time, digital assets need to be developed in a compliant manner, and governments or regions are exploring appropriate regulatory frameworks for digital assets. The authors of this book are senior practitioners in the Web3 field, with both a high global perspective and rich frontline practical experience. This whitepaper covers very critical security management, compliance, privacy, risk management frameworks and security practices in the digital asset space in a comprehensive and informative manner.

RigSec, as a professional digital asset custody solution provider, is honoured to participate in the white paper led by Amber Group to contribute to the healthy development of the industry.

The wave is here, let's work together.

Neilson Lei, CTO, RigSec

RECOMMENDATION VIII - ANCHAIN.AI

Web3 crypto assets, from 0 to a trillion-dollar asset class in just ten years, is a rarity in the history of human finance.

AnChain.AI was founded in 2018 in Silicon Valley, USA, when the crypto market capitalization was only ten million dollars, as a new fintech platform parallel to Wall Street. In just five years, we have been fortunate enough to stand on the wave of the Silicon Valley era, witnessing the Web3 crypto industry grow from grassroots savagery to being recognized by global financial institutions, and embracing regulatory compliance.

Web3 financial assets, such as Stablecoin, NFT, DeFi, is a very technical financial product category. We have been committed to solving two major Web3 security issues: Security and Compliance. Security and compliance are two sides of the same coin, closely linked:

1) Security is the inner workings of a Web3 encryption enterprise, including smart contract security, real-time monitoring, incident response and SOC security operations.
2) Compliance is a huge external force, from the countries regulated by AML, CFT, market manipulation, taxation and so on.

2023 is a watershed year for the Web3 security industry. With the Fed's interest rate hike and capital market cooling, the market is rationalizing and the regular army is entering the market. This market adjustment is favourable to the long-term trend of the industry.

- In terms of compliance, in 2023, the world's major economies, such as Europe, Japan, South America, the Middle East, Hong Kong, China, etc., have introduced cryptocurrency regulatory programs, such as MICA in Europe, VARA in the Middle East, CBDC in South America, etc.; U.S. governmental agencies such as the SEC, FINCEN, IRS, etc., have gradually clarified the industry's regulation. AnChain.AI has had the privilege of working with government agencies around the world to develop RegTech regulatory technology products. Because, compliance is the only way out for the Web3 crypto industry.
- On the security front, the international cybersecurity event RSA, for the first time in 2023, awarded the Innovation Sandbox Award to AnChain.AI's Web3SOC product. This is the first time in 18 years that RSA has recognized Web3 security. We look forward to seeing more outstanding Web3 security companies on the RSA Conference podium in the future.

For the past three years, Amber Group has been a valued client of AnChain.AI in the Asia Pacific region, and we have worked together to continually raise the bar on both security and compliance. AnChain.AI is honoured to contribute as a co-author to this informative and practical White Paper on Digital Asset Security, Compliance and Risk Control.

AnChain.AI and Web3's industry-leading partners are eagerly awaiting the dawn of a new financial era.

Victor Fang, Ph.D., CEO, AnChain.AI, San Francisco

ANCHAIN.AI

RECOMMENDATION IX - ANKURA

Ankura, a global independent expert services and consulting firm, provides end-to-end services and solutions to clients at critical inflection points related to resistance, crisis, performance, risk, strategy and transformation. We are honoured to have been involved in the whitepaper led by Amber Group.

As digital assets and cryptocurrencies continue to evolve and innovate, adherence to established standards and frameworks is critical to ensure security, transparency, and operations. For the digital asset industry, ISO (International Organization for Standardization) has established several standards such as ISO 27001 for information security management, ISO 27701 for privacy information management, ISO 23635 for governance guidelines for blockchain and decentralized ledger technology, and ISO 29151 for personal privacy protection. These standards provide comprehensive guidance on conducting audits, assessments, and compliance checks, including wallet security, data protection, and transaction integrity. Organizations can also leverage industry-specific frameworks, such as the Cryptocurrency Security Standard (CCSS), to ensure that their digital asset practices are in line with generally acknowledged security benchmarks. Such audits and assessments help identify vulnerabilities, enhance cybersecurity measures, and build trust among stakeholders.

Digital asset protection typically involves protecting cryptocurrencies, tokens and other digital assets from unauthorized access, theft or loss. Popular technologies in this field include key management, hot and cold wallet policies, multi-signature authentication, hardware security modules (HSM), and cryptography. In this whitepaper, we will share best practices for protecting digital assets from cyber-attacks, phishing, and insider threats, as well as insights into secure smart contract development and code auditing to prevent vulnerabilities.

The difficulty of identifying individuals involved in illegal activities, money laundering, or fraud in related cases involving digital assets continues to rise. Meanwhile, skills of investigation, tracing, and analysis of blockchain transactions are evolving as well, including identifying addresses associated with dark web markets, ransomware payments, or Ponzi schemes. In this whitepaper, we will discuss the challenges faced, the tools and techniques used, and the legal and ethical considerations involved in conducting such investigations. Sharing these experiences helps law enforcement agencies, regulators, and businesses better understand the changing landscape of cryptocurrency-related crime.

As digital assets and cryptocurrencies grow in popularity and personal data privacy acts continue to improve in various countries and regions, data privacy compliance becomes increasingly important. Maintaining user privacy, obtaining consent for data processing, and securely managing personal information in blockchain networks all face new challenges. Additionally, organizations should proactively address compliance and risks related to financial assets such as Anti-Money Laundering (AML) and Know Your Customer (KYC) to build user trust.

Ankura would like to take this opportunity to share our expertise and knowledge to jointly advance the results and enhance the understanding of digital asset practices, security measures, investigative techniques, and compliance strategies, to promote a more transparent and safer digital asset ecosystem.

Han Lai, Senior Managing Director, Ankura

I. PREFACE

1.1 BACKGROUND AND PURPOSE

Today's digital economy has become an important engine of economic growth, and in the digital economy, the development of digital assets represented by blockchain technology has become an unprecedented technological change. With the continuous development and application of blockchain technology, more and more industries have begun to explore how to apply it in practical scenarios, so as to realize more efficient, safer, fairer, and improved data exchange and value transfer with increased transparency. The era of digital assets with blockchain as the underlying technology has quietly arrived. After more than ten years of development, digital assets have gradually stepped into the era of moderate regulation from the era of barbaric growth, and have gradually entered into the public's view from crypto-punks and geeks' circles, so that a wider range of people can enjoy the dividends of the development of digital economy.

Digital assets are the oil and gold of the new era, both of which are a form of stored value, but in contrast, emerging digital assets face greater risks in terms of liquidity, price volatility, security, and so on. Since the birth of Bitcoin, an unprecedented "gold rush" has begun, with frenzied hacker groups, speculative and mismanaged businesses causing massive losses of user funds, bringing dramatic turbulence to the industry, and becoming a major obstacle to the entry of traditional industry talent, users, and investors into the digital asset space. With the introduction of global digital asset regulatory regulations and the formation of industry self-regulatory organizations, it will be expected to establish more efficient, safe, fair and improved industry norms with increased transparency, and digital asset enterprises committed to long-term development will usher in the spring in the era of compliance, and the obstacles to the large-scale popularization of digital assets will hopefully be effectively alleviated.

In this whitepaper, we explore the characteristics of the digital asset industry, identify its common risks and challenges, and introduce cutting-edge security, compliance, and risk-control solutions. We also provide insights and practical cases that serve as a reference for digital asset enterprises looking to build a framework that meets compliance and regulatory requirements while implementing the concept of "Responsible Technology." Our goal is to establish a new paradigm of digital trust that enables traditional industry talent, users, and investors to confidently enter and participate in the digital asset space.

1.2 INTENDED AUDIENCE

- Digital asset business leaders
- Digital asset regulators
- Enterprises exploring digital asset adoption
- Venture capital firms and insurers in the digital asset sector
- Cybersecurity experts in the digital asset space
- Readers interested in best practices for digital asset security, compliance, and risk management systems

This paper offers insights for a diverse readership with interests in the maturation of the digital asset industry. For enterprise leaders and regulators, it outlines pragmatic pathways to enhance the reliability and trustworthiness of blockchain-based financial systems. Cybersecurity practitioners will find an overview of cutting-edge techniques to harden digital asset platforms against theft and abuse. Investors and insurers will gain perspective on how prudent controls and compliance protocols can tame digital assets' notorious volatility. Overall, readers will discover how the latest security, compliance and risk management innovations are paving the way for digital assets to realize their immense potential through heightened stability and mainstream adoption.

II. OPERATIONAL OVERVIEW

2.1 BUSINESS RISKS IN THE INDUSTRY, DIGITAL ASSET BUSINESS CONCEPTS

Business risk in an industry refers to the risks that a company may face in the course of its operations in a particular industry. These risks may come from market competition, policies and regulations, and technological changes. For example, in terms of market competition, enterprises may face challenges from competitors such as price wars and new product launches; in terms of policies and regulations, the government may introduce new laws and regulations, which may affect the business model of enterprises; and in terms of technological changes, the emergence of new technologies may change the industry landscape, making it necessary for enterprises to undergo technological upgrading or transformation. Therefore, enterprises need to constantly pay attention to industry dynamics, assess risks and take corresponding measures to cope with them.

There are two concepts that need to be sorted out before we can understand the enormous difficulties and challenges that businesses are currently facing:

What are digital assets?

Digital assets are assets that exist in digital form and have value. Examples of digital assets include cryptocurrencies, digital securities, digital artworks, and more. These assets can be managed and traded using digital technology, with blockchain being a commonly used technology for secure trading and storage. As the industry evolves, new technologies such as big data are being integrated into digital asset businesses to enhance capabilities and value, creating exciting opportunities for investors and businesses alike.

What is the digital asset business?

Digital asset business refers to the business of utilizing digital technology to manage and trade digital assets. Digital assets may include cryptocurrencies, digital securities, digital artworks, etc. *(In order not to cause ambiguity, crypto-assets and virtual assets in the expression of this whitepaper are equivalent to digital assets, and cryptocurrencies and virtual currencies are equivalent to digital currencies)*. With the development of blockchain, big data and other technologies, the digital asset business is constantly evolving and innovating. For example, blockchain technology can be used to enable secure trading and storage of digital assets, and big data technology can be used to analyse market trends and provide investors with better investment advice.

What is a digital asset management company?

A digital asset management company is a professional organization that specializes in the management, trading and secure custody of digital assets for its clients. Digital assets include cryptocurrencies, digital securities, digital artwork, blockchain assets, etc. The responsibilities of a digital asset management company include providing services such as secure storage of digital assets, asset management and portfolio management, risk management, security management, technical support and other services to ensure that clients' digital assets are optimally utilized and protected.

At present, mastering rich high-value data resources is increasingly becoming a prerequisite and guarantee for enterprises to seize the initiative for future development, and making full use of new digital technologies to drive the transformation of business models and the development of business strategies is the core essence of enterprise digital transformation. How to systematize digital asset management, apply security control measures to the enterprise's digital assets, and extend the resilience and robustness of digital assets have brought great challenges to enterprise management.

2.2 GLOBAL OVERVIEW OF DIGITAL ASSET MANAGEMENT

Governments around the world are busy drafting regulatory frameworks for digital assets. A clear and rational regulatory framework is key to the future development of the digital asset market. For example, Global Digital Finance (GDF) is leading the way in developing the most comprehensive code of conduct on digital assets. Nearly 75 companies around the world have committed to the GDF code of conduct through a self-certification process.

However, the process of digital asset regulation does not develop in a linear fashion, rather it is convoluted and fluid. The 2019 survey found that the top five regulatory challenges that exist today are:

1) Inconsistent cross-border regulatory guidance;
2) Unclear regulatory boundaries;
3) Not all market participants are regulated;
4) Insufficient proactive cooperation with regulators;
5) Regulatory actions are not authorized by the legislative framework.

National and local governments also have different attitudes and approaches to regulating digital assets.

In the United States, digital assets are categorized as ancillary assets, virtual currencies, payment-based stablecoins, commodities, and securities, with different emphases on the regulation of different types of digital assets. The bill has specific, agency-specific requirements for the issuance of digital assets and related activities, such as publicly disclosed information and how funds are managed. U.S. President Joe Biden officially signed the Digital Assets Executive Order on March 9, 2022, and released the full text on the official website of the U.S. White House. The executive order details the framework for U.S. regulatory action on digital assets in a number of areas, including policy, objectives, coordination among U.S. government agencies, measures to protect consumer investors and businesses, promoting financial stability, reducing systemic risk, limiting illicit finance, and promoting international cooperation and U.S. competitiveness. The main objectives of the Executive Order include protecting consumers, investors, and businesses, protecting financial stability, reducing systemic risk, mitigating illicit financial and national security risks posed by the misuse of digital assets, strengthening U.S. leadership in the global financial system as well as in technological and economic competitiveness, facilitating access to safe and affordable financial services, and supporting technological advances that promote the responsible development and use of digital assets .

In Singapore, the Monetary Authority of Singapore (MAS), as the financial regulator in Singapore, it has promptly indicated its regulatory attitude and introduced a series of digital asset regulation-related policies in response to the wave of digital asset investment. The Singapore government passed the Payment Services Act (PSA) on January 14, 2019, which brings digital payment token services into the scope of payment license regulation. Under the Act, companies providing digital payment token services are required to obtain a license issued by MAS and comply with the PSA's regulations relating to anti-money laundering and counter-terrorist financing. In addition, the MAS

has issued a Guide to Digital Token Offerings, which was revised on May 26, 2020. The Guidelines stipulate that digital tokens will be regulated by the MAS if they are Capital Markets Products (CMP) under the Securities and Futures Act (SFA), and that Capital Markets Products (CMP) encompasses securities, bonds, derivatives contracts, collective investment CMPs include securities, bonds, derivatives contracts, collective investment schemes, etc.

In Hong Kong, the approach to digital asset management is also evolving. The Hong Kong Government issued a "Policy Declaration on the Development of Virtual Assets in Hong Kong" on October 31, 2022, which aims to strengthen Hong Kong's regulatory regime to combat money laundering and terrorist financing, so as to promote the development of Hong Kong into an international virtual asset centre. To this end, the Hong Kong Legislative Council passed the latest amendments to the Anti-Money Laundering and Counter-Terrorist Financing Ordinance, which formally implements the new Virtual Asset Service Provider Licensing Regime (VASP Regime) with effect from June 1, 2023. This means that all centralized virtual asset exchanges operating in Hong Kong or actively promoting their services to Hong Kong investors will need to be licensed and regulated by the Securities and Futures Commission (SFC). This initiative is conducive to the establishment of an effective regulatory regime for combating money laundering and terrorist financing, in line with relevant international requirements, and will help consolidate Hong Kong's position as an international financial centre. For virtual asset exchanges, a comprehensive and balanced regulatory framework can protect investors and promote responsible and sustainable industry development.

In the United Kingdom (UK), it is also open to digital asset (referred to as crypto asset) business providing a protective and well-structured regulatory framework which is considered more measured in their response and enforcement than other regulatory regimes including the SEC in the US. The Financial Conduct Authority (FCA) requires crypto exchanges and other businesses carrying crypto asset activities in the UK to register with them meeting strong Anti-Money Laundering & Countering the Financing of Terrorism (AML & CTF) requirements for Virtual Asset Service Providers wishing to operate in the UK. The FCA is also introducing tougher roles on marketing Crypto assets. These rules require crypto asset firms to ensure that people have the appropriate knowledge and experience to invest in crypto. Those promoting crypto assets must also put in place clear risk warnings and ensure adverts are clear, fair and not misleading. From October 2023, those selling to consumers must also offer a cooling-off period for first time investors. Recent cases around crypto have put the UK at the forefront of disputes legislation both as a crypto currency exchange and as a victim of crypto related crime. Legally tested tools including new disclosure gateways, Norwich Pharmacal and Bankers Trust Orders are being used and tested in the UK courts. Some examples include: *AA v Persons Unknown*, *Ion Science v Persons Unknown*, *Fetch.ai Ltd & another v Persons Unknown*, *Tulip Trading Limited v Bitcoin Association for BSV ar*.

In the European Union (EU), European regulation is also maturing with the introduction of Markets in Crypto Assets (MiCA) which is a sound legal framework for crypto asset markets to develop within the EU. This will apply to any person providing digital (again referred to as "crypto") asset services or issuing crypto assets in or into the EU. It will not apply to security tokens already subject to existing EU regulatory regimes and will also not apply to Central Bank Digital Currencies (CDBC) but places significant requirements on global stablecoins.

2.3 DIGITAL ASSET BUSINESS CHARACTERISTICS

Digital assets are various values and interests that exist in digital form. They can be digital currencies (e.g., Bitcoin, Ethereum), digital securities, digitized artwork, virtual land, game props, etc. The existence and transactions of digital assets are based on blockchain technology, encrypted and verified by cryptographic algorithms. Its main types include:

- Cryptocurrencies: such as Bitcoin and Ethereum, are digital currencies that use cryptography to enable secure transactions;
- Tokens: digital assets that represent some kind of entitlement, physical object or service that can be managed and traded through smart contracts;
- Digital Securities: securities in digital form, such as stocks, bonds, options, etc.;
- Decentralized Finance (DeFi) Assets: financial instruments built on blockchain technology, such as lending agreements and stablecoins.

An important business in digital assets is crypto assets, which are encrypted and verified based on cryptography technology to achieve decentralized transactions and management with the support of blockchain technology. Crypto assets commonly have the following characteristics:

- Decentralization: the trading and management of crypto assets does not rely on a central authority, but rather on the consensus algorithms of the nodes in the blockchain network. This means there is no single point of control, reducing the risk and vulnerability of the system;
- Irreversibility: Once a transaction of a crypto-asset is confirmed and recorded on the blockchain, it cannot be undone or tampered with. This ensures the security and trustworthiness of the transaction;
- Programmability: The smart contract function of crypto assets gives them more application scenarios and flexibility. Through smart contracts, automated transaction execution, conditional payments, distribution of digital assets and other functions can be realized;
- Privacy: Transactions in crypto-assets are usually anonymous, and the identities of the participants can be encrypted and decrypted using public and private keys to protect the user's privacy;
- Globalization: The trading and transfer of crypto assets is not limited by geographic location, allowing for cross-border transactions and asset flows. This provides greater convenience and opportunities for financial and commercial activities on a global scale.

While traditional finance often relies on centralized institutions and legal systems to ensure the security and compliance of transactions, crypto assets achieve these goals through cryptography and blockchain technology. The anonymity, decentralization and irreversibility of crypto assets thus make them of great potential and innovation in the digital economy and finance. You can see the main differences between traditional finance and crypto assets include:

- Centralized vs. Decentralized: Traditional financial systems are usually controlled and managed by centralized institutions (e.g. banks, stock exchanges). Crypto assets (e.g. Bitcoin, Ether), on the other hand, are based on decentralized blockchain technology, where there is no centralized institution to control and all transactions and verification are done by multiple nodes in the network;
- Confidentiality vs. Transparency: In traditional financial systems, transaction and account information is usually private and accessible only to certain participants. In contrast, transaction and account information for crypto assets is public and can be viewed and verified on the blockchain;
- Real names vs. anonymity: In traditional financial systems, the identities of participants are usually known, requiring identity verification and KYC (Know Your Customer) procedures. Crypto-asset trading, on the other hand, can maintain a certain degree of anonymity, where participants can be identified with a key rather than their real names;
- Transaction speed and costs: In traditional financial systems, cross-border transactions can take days and involve high transaction fees and intermediaries. Crypto-asset trading allows for fast peer-to-peer transactions with lower transaction costs;
- Legal and regulatory: Traditional financial systems are regulated by national laws and regulatory bodies. In contrast, the legal and regulatory environment for crypto-assets is still evolving, with varying attitudes and regulations in different countries.

In summary, the emergence of crypto-assets has brought innovation and opportunities to the financial sector, but also challenges and risks. While crypto assets offer more investment options and efficient trading methods, their decentralized nature and market volatility also bring security considerations. The security of crypto assets has simultaneously become a topic of focus, including risks in terms of market manipulation, security breaches and fraud, as well as uncertainty in the regulatory and legal environment. Ensuring the security of crypto-assets and investor protection is therefore a pressing issue today.

Amber Group -
committed to building a more secure and reliable digital asset ecosystem

Amber Group is a leading crypto-asset financial services provider that offers clients a comprehensive suite of solutions to meet their buying and selling needs for crypto-financial products. Its range of services includes asset management, yield enhancement, trade execution, collateralized lending, and market making, as well as risk management and liquidity access.

Located at the heart of the global crypto-financial market, Amber Group leverages its talent, capital, and state-of-the-art infrastructure to deliver innovative products and solutions that help users stay competitive and optimize their returns in an ever-changing market. The company combines high technology such as artificial intelligence, big data, and blockchain with quantitative research to provide cutting-edge services that cater to various client segments.

Its core businesses encompass:

1) Digital wealth management services for high net worth individual investors and family offices;
2) Crypto-native liquidity services for institutional clients such as exchanges, token issuers, funds, and cryptocurrency project owners;
3) One-stop-shop crypto-financial infrastructure-as-a-service and security compliance solutions for the digital asset industry.

III. SECURITY RISKS AND CHALLENGES IN THE AGE OF DIGITAL ASSETS

In this chapter, we come together to take you through four common security risks and challenges experienced during the development of digital assets, and explore security, compliance and risk control solutions for the digital asset era together from the vision of an industry-leading digital asset security compliance company.

3.1 SECURITY CHALLENGE I: THE CHANGING DYNAMICS OF THE CHAIN AND THE UBIQUITY OF SECURITY THREATS

In 2014, Vitalik Buterin founded Ethereum, an open blockchain-based platform that allows users to create and deploy smart contracts which execute and interact with other smart contracts automatically without the need for centralized institutions or trusted parties. It brought paradigm innovations like smart contracts, decentralized applications (DApps), and decentralized autonomous organizations (DAOs), kicking off a wave of blockchain ecosystem innovation based on on-chain smart contracts. From DeFi and NFTs to GameFi, the Metaverse and DAOs, the digital finance revolution driven by Ethereum is changing the world.

With the advancement of blockchain technology and applications, smart contracts have become an essential part of blockchain apps. However, various security issues have increasingly emerged in the development and operation of smart contracts. Hacks exploiting vulnerabilities in smart contracts have caused tremendous losses across the blockchain industry.

According to data from SlowMist, as of 2023, various blockchain hacking attacks have resulted in around $30 billion worth of cryptocurrency assets stolen. These attacks targeted blockchain infrastructure like DeFi protocols, centralized exchanges, decentralized exchanges, and cross-chain bridges.

3.1.1 INDUSTRY PAIN POINTS AND SECURITY THREATS

Smart contracts have characteristics like on-chain transparency, decentralization, programmability, security, low cost, and immutability, making them highly promising across many fields. However, the crypto assets controlled by those smart contracts are also directly exposed to hackers such that a successful exploit of vulnerabilities can lead to irrecoverable losses.

1) **Assets on-chain are easy targets:** Smart contract assets are usually stored as cryptocurrencies. Operations like claiming, transferring, and approving all happen on-chain, allowing hackers to easily scan for potential vulnerabilities to target.
2) **Human-written code inevitably has bugs**: Smart contracts are manually coded, leading to common errors like reentrancy, access control issues, integer overflows, etc.
3) **Composability introduces unknown risks**: In the DeFi ecosystem, protocols often run other protocols and smart contracts, potentially causing unknown risks.
4) **Key management and permission errors**: Many smart contracts have administrator roles with control permissions. Lost private keys or improper administration can lead to financial risks.

However, as the ecosystem matures, security-focused firms like Trail of Bits, ConsenSys Diligence, OpenZeppelin, CertiK, BlockSec, SlowMist, and AnChain.AI now provide smart contract auditing, pre-launch scanning, monitoring, and security response. Their involvement has reduced incidents, minimized losses, and boosted reliability, playing a crucial role.

Still, the rapid growth with prolific new chains, wallets, bridges, and DeFi can lead to weak security practices. Projects often launch or upgrade without audits, introducing potential issues that threaten long-term stability.

3.1.2 STORY 1: THE DAO EVENT LEADS TO ETHEREUM HARD FORK

On June 17, 2016, a hacker successfully exploited a reentrancy vulnerability in The DAO's smart contract to execute a reentrancy attack, permanently draining over 1.5 million ETH (worth around $500 million at the time) within hours. Specifically, the hacker recursively called The DAO's refund function to trick it into dispensing exorbitant "rewards."

Faced with this unprecedented hack, the Ethereum community submitted a fork proposal EIP 160 to hard fork the blockchain, essentially reverting the hack by hardcoding the stolen funds back to victims. This also split Ethereum into another project called Ethereum Classic (ETC) as miners opposed to the fork continued on the original chain. Although the measures successfully resolved the crisis, they also sparked huge controversy regarding Ethereum's governance, values and decentralized collaboration.

This attack exemplified the dangers of reentrancy vulnerabilities in Ethereum smart contracts. It prompted developers, communities and regulators to prioritize smart contract security, auditing and internal controls, catalysing rapid evolution of vulnerability patching and security governance in blockchain. The event serves as an important reminder of the need for comprehensive smart contract and blockchain auditing.

Industry Thoughts:

Before interacting with smart contract projects, digital asset managers should thoroughly review and test them including code reviews, vulnerability scanning, transaction testing, and other detection and verification. This aims to ensure stability, reliability and safety. Firms should also closely collaborate with security partners to jointly assess risks and response strategies. Such comprehensive security reviews aim to uncover potential vulnerabilities and issues before launch, assisting projects with remediation to provide users with secure and reliable products and services.

3.1.3 STORY 2: ETHEREUM CLIENT PARITY MULTISIG VULNERABILITY, OVER $150 MILLION WERE AFFECTED

In July 2017, the Ethereum client Parity released a multisig wallet contract library, aiming to provide a convenient and secure Ethereum multisig wallet solution. However, the contract had a severe access control vulnerability. The flawed contract logic allowed anyone to call the self-destruct function, permanently locking funds in the contract.

In November 2017, this vulnerability was accidentally triggered by an anonymous user, resulting in over 513,743 Ether being locked (worth $152milion in total at the time). Parity tried to recover the frozen funds via a hard fork but this proposal did not gain support from the Ethereum community.

This event exposed that any minor smart contract logical design flaw in permissions could lead to irreversible severe consequences. It demonstrated the importance of comprehensive security audits before deployment. Once a problem occurs, it is extremely difficult to change the decentralized consensus and recover losses.

The incident also served as an important caution for developers to carefully design smart contract access controls and thoroughly test contracts prior to deployment, given that any vulnerabilities exposed after launch can lead to irreversible damage

Industry Thoughts:

In digital asset fields, asset management firms should recognize the importance of full lifecycle security for contract deployment. Pre-launch security audits and code testing are indispensable steps. Effective simulation testing should be conducted on production contracts to eliminate potential risks. While extensive human resources are required, these vulnerability assessments are imperative due to the irreversibility of flaws. Therefore, this level of security awareness should be universally acknowledged and adopted across the industry.

3.1.4 STORY 3: PHISHING ATTACKS ON OPENSEA NFT MARKETPLACE USERS

On February 19, 2022, hackers used a phishing email attack to steal 254 NFTs, including valuable Decentraland and Bored Ape Yacht Club collectibles, from an OpenSea user.

Specifically, the hackers sent the target user a spoofed email posing as OpenSea, asking them to approve a smart contract and provide sensitive information like social media logins and API keys. If the user did not exercise caution and signed the Approve transaction, it would lead to irreversible crypto asset loss.

This incident exposed insufficient awareness of cybersecurity risks among crypto users, including inability to identify spoofed trusted certification links, lack of format checking and identity verification, and over-trusting unverified information sources like social media.

With risks and vulnerabilities frequently emerging in areas like NFTs, educating users to enhance self-protection awareness is crucial. Developers should also proactively implement security

precautions like identity authentication to restrict malicious attacks and policy violations, building healthier, more secure and efficient digital trading platforms.

Industry Thoughts:

The security of user assets is paramount for companies providing digital asset management platforms. Platform providers should implement robust security systems encompassing monitoring, internal audits, and 24/7 incident response to fully safeguard user assets under any circumstances. Achieving this level of security should be the top priority industry-wide.

3.1.5 INDUSTRY SECURITY SOLUTIONS PRACTICES

3.1.5.1 WEB3 AND BLOCKCHAIN SECURITY SYSTEM PRACTICES

To effectively mitigate the uncertainties and potential risks associated with on-chain smart contracts, it is vital to establish a robust and comprehensive Web3 and blockchain security risk management system. At Amber Group, our security team consists of experts who excel in various domains crucial to this effort, such as Web3, red team/blue team tactics, financial compliance, data privacy, and overall risk assessment. Below are some practices this team undertakes to maintain robust security through our risk management system and control measures:

1) Regular smart contract audit: Conduct regular security audits on popular or critical smart contracts to identify vulnerabilities and risks, provide timely recommendations to developers, and warn users of potential dangers.
2) On-chain risk monitoring: Build 24/7 on-chain risk monitoring leveraging blockchain and data analytics to scan network activity, smart contract invocations, fund flows etc. in real-time to detect potential threats or anomalies.
3) Ongoing security research: Maintain in-house security team or participate in industry activities to stay abreast of emerging security issues and provide valuable insights for business stability.
    - Fuzz testing: Fuzz testing is currently the most effective automated testing paradigm for finding software bugs. Many zero-day vulnerabilities have been discovered in blockchain clients recently through fuzzing, e.g. [1] Smart contracts are harder to fuzz due to complex logic combinations, so manual audits are still mainstream. Fuzzing smart contracts requires modelling them as complex systems, mapping function relationships, mutating via known flaws etc. to get accurate results. Extracting states or simulating states is needed as blockchains have different states over time. This field is still exploratory and Amber Group is actively developing solutions based on our fuzzing expertise [2, 3].
    - CTF/Hackathons: With the fast-changing Web3 landscape, staying updated is crucial. Security teams can regularly participate in events like CTFs and hackathons to quickly gain relevant skills and knowledge, and validate alignment with industry frontiers.

For example, our team placed 6th in Paradigm CTF 2022 and won 3rd in AnChain.AI 2022 IHackNFT smart contract CTF. We have excelled in other events by MoveBit, Numen Cyber, ETHTaipei, Flashbots, etc.

- Vulnerability Research: There are abundant 0-day and N-day vulnerabilities in Web3. The security team should regularly evaluate and penetrate Web3 technologies/products, and responsibly disclose vulnerabilities to help projects mitigate potential losses. For example, we discovered and reported vulnerabilities in NFT platform Position Exchange, helping them avoid potential damage and receiving a bug bounty [4].

  We have discovered 0-days including *"CVE-2022-48423"*[5], *"CVE-2022-48424"*[6], *"CVE-2022-48425"*[7], *"Dinosaur Eggs' LiquidityPool Loophole Explained"*[8] and *"Strips Finance's Price Manipulation Vulnerability Explained"*[9] and reproduced over 100 N-days, notably "*Mai Finance's Oracle Manipulation Vulnerability Explained*"[10].

- OpenSource Contribution：Blockchain technology, from the underlying node to the upper-level smart contract virtual machines, is built upon the principle of open-source verifiability, which ensures that security experts and ethical hackers can efficiently identify any potential problems, vulnerabilities, and bugs. As part of their efforts to maintain robust security, security teams should actively participate in various open-source communities and projects, providing technical support, product recommendations, and contributions to help improve the overall security and effectiveness of these projects.

  Currently, Amber Group's Papora fuzz testing framework, which has been recognized by Black Hat and WOOT, is available on Github as an open-source project [11].

3.1.5.2 WEB3 PROJECT LIFECYCLE PROTECTION PRACTICES

As Web3 projects sprout rapidly, smart contract vulnerabilities also emerge across the entire lifecycle. For example, potential design flaws due to developers' weak security awareness during development, potential security issues caused by discrepancies between development and production environments during deployment, and new bugs arising from complex logic after launch.

The security issues of Web3 projects are like the buckets theory - the overall security of a system depends on its weakest component. While necessary security audits of smart contracts are important, comprehensive business design before auditing, monitoring and maintenance, and

incident response after auditing are also crucial. Even with multiple levels of security protection, if the weakest link fails, the assets of the entire system may be at risk.

Based on Amber Group, BlockSec and SlowMist's security architecture and hands-on experience throughout the Web3 project lifecycle, here are some suggested actions for digital asset management companies' security teams:

3.1.5.2.1 WEB3 PROJECT LIFECYCLE SECURITY PROTECTION METHODS

3.1.5.2.1.1 DEVELOPMENT PREPARATIONS

Before developing a Web3 project, preparation work in various aspects needs to be done well:

1) Requirements analysis document: Including collecting user requirements, analysing functional requirements, summarizing non-functional requirements, security and privacy risk assessments, etc. to form a requirements document;
2) Design analysis document: Including designing system architecture, contract modules, descriptions of key function features, security and privacy mechanisms, client interactions, etc., eventually forming a development design document;
3) Process planning document: Including analysing business requirements, designing business process flowcharts, defining roles and permissions, designing business exception handling, and other specific business process specifications, eventually forming business process documentation.

3.1.5.2.1.2 DEVELOPMENT PROCESS REQUIREMENTS

During the development of Web3 projects, it is important to follow some development specifications, including code specifications, security specifications, testing specifications, deployment specifications, etc. The following are some incomplete examples (referencing the Web3 project security practice requirements document open sourced by SlowMist):

1) Key smart contract secure coding requirements
   - Ensure contracts are developed as reusable libraries, referencing OpenZeppelin etc.
   - Use SafeMath or >=0.8 compiler to avoid overflow issues.
   - Follow Solidity naming and visibility conventions.
   - Explicitly declare function and variable visibility as public/private.
   - Explicitly assign return values instead of relying on defaults.
   - Provide complete and standardized comments for functions and parameters.
   - Check return values properly for external calls like transfer/send etc.
   - Avoid using unknown libraries, test new functions for safety.
   - Use private visibility by default unless necessary.
   - Validate inputs properly using require()/assert().
   - Split contracts into multiple files to reduce complexity.
   - Use tools like Slither/MythX to aid in auditing code.
   - Restrict read-only access for databases to prevent tampering.

- Consider reentrancy risks thoroughly for external calls.
- Avoid using on-chain block data as the random number source.
- Ensure randomness generation and usage accounts for rollback attacks.
- Ensure external contract interactions are compatible, e.g. ERC-777, ERC-677, ERC-721 for reentrancy-safe tokens.
- Record execution state via events in critical flows for analysis if needed.
- Include global and core business emergency stop switches for timely loss mitigation.

2) Test case coding requirements
   - Write sufficient test cases (95%+ coverage) covering all functions and edge cases.
   - Regularly deploy test cases to testnets for testing.
   - Automate test cases as much as possible, avoid relying on manual testing.
3) Basic security configuration requirements
   - Test contracts on isolated private networks first.
   - Use separate wallet addresses for development and testing, do not mix with production.
   - Store necessary private keys and config files securely.
   - Reset contract state before new tests to avoid state pollution.
4) Front-end security configuration requirements
   - Use wallets like Metamask to connect real user crypto assets.
   - Validate and sanitize input data to prevent XSS and SQL injection attacks.
   - Rate limit contract interaction interfaces to mitigate DDOS risks.
   - Minimize use of third-party JavaScript libraries and permissions.
   - Ensure cookies related to auth and credentials are configured with HttpOnly, Secure, Expires and SameSite flags.
   - Set X-Content-Type-Options to defend against browser sniffing risks.
   - Use integrity checks on third-party resource references to prevent impacts from compromised sources.
5) Back-end security configuration requirements:
   - Use dedicated database instances, do not mix production and test data.
   - Set time-limited validity periods for database accounts, whitelist allowed IP addresses, restrict access sources, etc.
   - Encrypt database connections using TLS/SSL to increase transport security.
   - Set alerts to monitor anomalous database connections and operations.
   - Regularly review database operation logs to check for any suspicious activities.
   - Stay up-to-date on database security notices, proactively apply security patches.

3.1.5.2.1.3 ITEMS FOR PROJECT DEPLOYMENT PROCESS

When preparing to release an official version of a Web3 project, it's crucial to follow a comprehensive set of deployment procedures. These procedures ensure that the project is launched smoothly and effectively, with minimal risk of errors or issues.

1) **Code freeze:** Freeze code 1-2 days before release, only allow urgent bug fixes.

2) **Unit testing:** All features must pass comprehensive unit testing, aim for 100% coverage.
3) **Regression testing**: Conduct regression testing on core flows before release, verify it passes.
4) **Security audits:**
    - Perform full security audits on frozen code.
    - Delay release for serious/high/medium severity findings until fixed.
    - Cross-validate with 2+ audit firms.
5) **Performance testing:** Complete stress testing to ensure stability under high concurrency.
6) **Release:** Generate release report confirming sufficient testing.

3.1.5.2.1.4 PROJECT OPERATION MONITORING

To ensure sufficient security for Web3 projects during operations, security and DevOps teams need to conduct monitoring and operations in a "comprehensive" manner. Based on multiple successful experiences in on-chain defense against hacker attacks, the BlockSec security team has summarized the following recommendations:

1) **Ensure a secure and reliable runtime environment:**
    - Harden server SSH configurations; deploy web application firewalls to filter input and output; deploy RASP to detect runtime attacks.
    - Isolate development, testing, and production environments; prohibit external network access to production environments.
    - Secure open source components via safe compilation, strengthen database account and password security; reduce unnecessary component functionality to minimize attack surface.
    - Regularly check server operations, system patches and component security updates.
2) **Implement robust internal controls:**
    - Establish sound private key storage and management mechanisms.
    - Regularly review access controls for sensitive systems like admin panels.
    - Enforce periodic password changes and strengthen overall password access policies.
    - Detect anomalies via event logs and other means.
3) **Strengthen project code security reviews:**
    - Ensure code provenance control, e.g. monitor related GitHub accounts and update operations.
    - Conduct manual and automated security analysis and audits to identify potential vulnerabilities and issues.
4) **Build comprehensive on-chain monitoring and protection:**
    - Timely monitor and collect on-chain and pending transactions.
    - Detect and handle attack transactions; accurately identify and block major attacks or pause contracts.
    - Monitor anomalies like critical contract calls, privilege changes, large transfers by new privileged accounts, liquidity removals, oracle price changes, etc.
    - Monitor interactions between high risk addresses and target contracts.

3.1.5.2.1.5 INCIDENT RESPONSE HANDLING FOR PROJECTS

Here are some incident response tips summarized by the SlowMist team, who have extensive experience in tracking hacked assets, based on multiple asset tracking cases:

1) Security Monitoring and Alerting:
   - Detect security incidents via deployed monitoring systems and promptly alert and escalate.
   - Define systematic incident response plans and assemble an incident response team.
2) Execute Loss Mitigation and Blocking Measures:
   - Promptly pause affected contracts to mitigate losses.
   - Attempt to block ongoing attacks via front-running countermeasures.
   - Notify communities and users to avoid further harmful interactions.
   - Provide emergency capabilities like account freezes, fund isolation, transaction rollbacks.
3) Stolen Asset Tracking Process (Typically with the Help of Security Firms):
   - Assess tracing feasibility based on factors like fund transfers, hacker patterns/profiles, law enforcement involvement, attribution to known hackers.
   - Maintain communication to manage expectations on recovery odds.
   - Monitor stolen funds and watch for transfers, especially to exchanges/wallets for freezing.
   - Trace on-chain transfers and identify hacker patterns from snapshots, IPs etc. Output tracing reports.
   - Profile hackers via timelines and behaviours like laundering methods and tools.
   - Assist law enforcement with on-chain analysis, exchange subpoenas, technical support throughout investigations.
   - Leverage specialized tracing tools like MistTrack, Chainalysis, MetaSleuth.

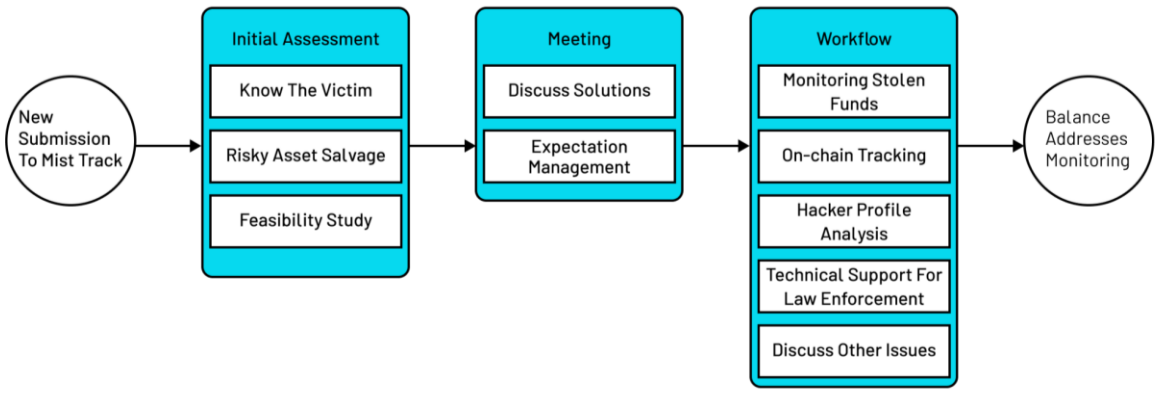

Figure: SlowMist asset tracking workflow [12]

4) Remediate Security Issues and Conduct Retrospective:
    - Analyse root causes of incidents and summarize response lessons learned.
    - Propose recommendations to improve emergency plans and processes.
    - Continuously provide active support to third party security firms and law enforcement for ongoing asset tracing efforts.

3.1.5.2.2 PRACTICAL WEB3 FULL LIFECYCLE SECURITY PROTECTION CASE STUDIES

3.1.5.2.2.1 AMBER GROUP CASE STUDY - PROFANITY "VANITY ADDRESS" PRIVATE KEY CRACKING ATTACK

On September 20, 2022, major crypto market maker Wintermute was hacked, losing $160 million. The root cause was a leaked private key for Wintermute's 0x0000000fe6a514a32abdcdfcc076c85243de899b address, which was a "vanity address" generated by the Profanity tool. Hackers successfully cracked the private key.

Amber Group's security team believes this exploit targeted an ecosystem weak point that could lead to sustained attacks. They have determined that any vanity address generated by a tool called Profanity has a probability of being cracked. To validate this vulnerability, the security team reproduced the Profanity bug exploit using a MacBook with an M1 chip and 16GB RAM. Within a span of less than 10 hours, they successfully generated a dataset that could be utilized to crack various addresses. In practice, we were able to crack the private key of 0x0000000fe6a514a32abdcdfcc076c85243de899b from scratch within 48 hours, through 36 hours of design and implementation, 10 hours of pre-computation to build the datasets, and a final 40 minutes to actually crack the private key based on our pre-computed data.

Our analysis showed Profanity uses a 32-bit random device seed (C++ std::random_device) to generate keys. To generate a 256-bit private key, this seed is input into the deterministic pseudo-random number generator mt19937_64. Thus, obtaining the seed is equivalent to obtaining the private key. Since there are only 2^32 possible seeds, and each iteration is reversible, private keys can be reverse-engineered from Profanity-generated public keys.

Profanity is an open-source custom private key generator that creates addresses with identifiable names/numbers. It is used to generate special EOA addresses to save gas for high-frequency contract invocations. However, any upstream generator vulnerabilities compromise all downstream users. Clearly, private key generation is the most upstream and overlooked part of key management lifecycles. After identifying the issue, Amber Group's security team studied Profanity's ecosystem usage and warned of risks through multiple channels, helping Web3 projects eliminate risks from the source. [13]

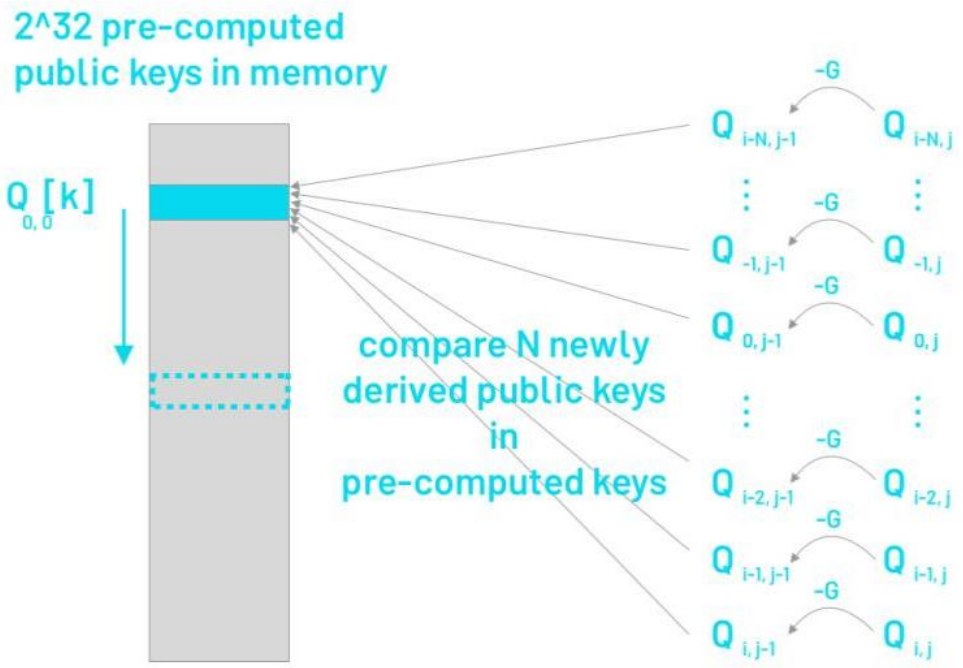

Figure: Compare N newly derived public keys in pre-computed keys

In the preparatory work for web3 project development security practices, we mentioned that developers should pay attention to the smart contract coding standard requirements. The Profanity case is precisely a problem in the acquisition and use of random numbers. Because the selection of the random number seed is limited to 2^32, which is an insufficient condition for a 256-bit private key, it gives hackers the possibility to exploit this vulnerability to carry out attacks. If developers can fully enclose testing in the test environment before the project goes online, and timely adjust the seed selection range, it can also avoid such vulnerabilities threatening the products in the production environment.

3.1.5.2.2.2 ANCHAIN.AI REAL-WORLD CASE - MILLION DOLLAR DEFI DARK FOREST INCIDENT RESPONSE

"RESCUING SCHRODINGER'S CAT IN DEFI'S DARK FOREST."

In November 2020, the AnChain.AI team, Web3 Incident Response, assisted a San Francisco cryptocurrency VC fund in successfully recapturing millions of dollars of DeFi investment money from hackers, taking the Silicon Valley FinTech community by storm. It became the ground-breaking first success story of exploring the "Dark Forest of DeFi" to recover stolen funds for a VC client.

"The Dark Forest," derived from Liu Cixin's famous science fiction novel "Three Bodies," refers to the "Law of the Dark Forest" described in the book: In the Dark Forest, others represent a perpetual threat, as the law holds that any life that reveals its own existence will soon be annihilated.

In August 2020, the "Dark Forest of Ether" was proposed by Paradigm's Dan Robinson and white-hat hacker Samczsun.[14] The Dark Forest is a "dark forest" where the world's most powerful people can be destroyed.[14]

SAN FRANCISCO, USA, November 3, 2020, 8:00 PM - The AnChain.AI team received an urgent request for help from a cryptocurrency VC in San Francisco. The VC has just been subjected to a phishing attack that leaked the keys to the Metamask wallet.

The hackers have stolen 4 ETH and the wallet's book balance has been zeroed out. The hackers do not seem to have noticed that the wallet is at a DeFi doing pledge staking liquidity mining for $1.2 million worth of USDC ERC20 stablecoins!

These pledged assets are like Schrodinger's Cat: lost in a quantum state, locked in a sealed, cold, hard box case, as in the Copenhagen quantum science experiment. As a result, only the moment the box is opened (and the stolen wallet connected) does one know if the collateralized assets are safe or not:

- Assumption 1: The hacker is informed and may be waiting for DeFi to yield more before doing so.
- Assumption 2: The hacker is unaware. But if we interact with Ether, sooner or later the hacker will find out about these encumbered assets, and maybe curiosity killed the cat.

Many users first come to AnChain.AI after having their cryptocurrencies stolen, seeking to possibly recoup losses via AnChain.AI's blockchain security and compliance services.

Less than 10% of our clients are lucky enough to recover their assets, while the rest report to Law Enforcement, a local and international law enforcement agency, with our assistance, patiently waiting for the hackers to expose themselves or to launder their money on compliant exchanges.

This novel DeFi theft case presents us with a new opportunity. If we play this game right, millions of dollars lost and found can happen.[15]

The AnChain.AI team quickly guided the client through the Web3 incident response:

Step 1: Site protection and blockchain forensics

- Disconnect from the Internet, turn off your computer, and contact us using a new computer and phone.
- Do not share private keys with anyone, including security companies.
- Do not connect your wallet to any DeFi products or websites.

Step 2: Hacker profiling

"If you know your enemy and know yourself, you will never be in danger." The key to hacker profiling is to gather intelligence, understand their motivations and behaviours, and take appropriate defensive measures.

We opened AnChain.AI's CISO blockchain investigation platform and found that the hacker's Ethereum address is relatively active, and that at least 5 victims have already fallen into the hacker's phishing scam trap.

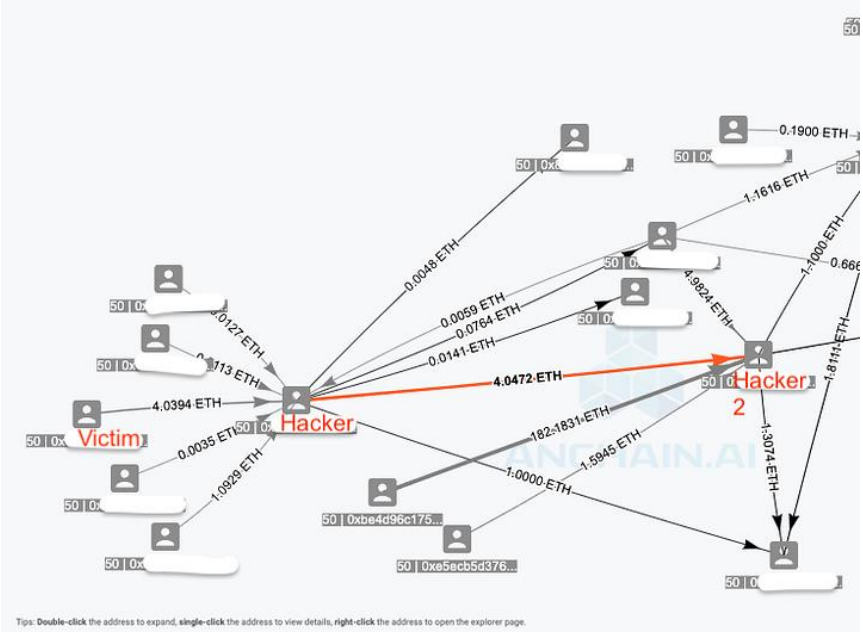

Figure: Hacker profiling

The Web3 blockchain is not like a web server that can track alias fingerprints such as IP addresses and browser user agent strings. The Ethereum blockchain can only anonymously record wallet addresses and the state of smart contracts.

By querying the AnChain.AI Web3 big data platform, we statistically analyse the hacker's historical transaction behaviour, and come up with a clear probability density function of the active time, inferring that the hacker may be in East Asia.

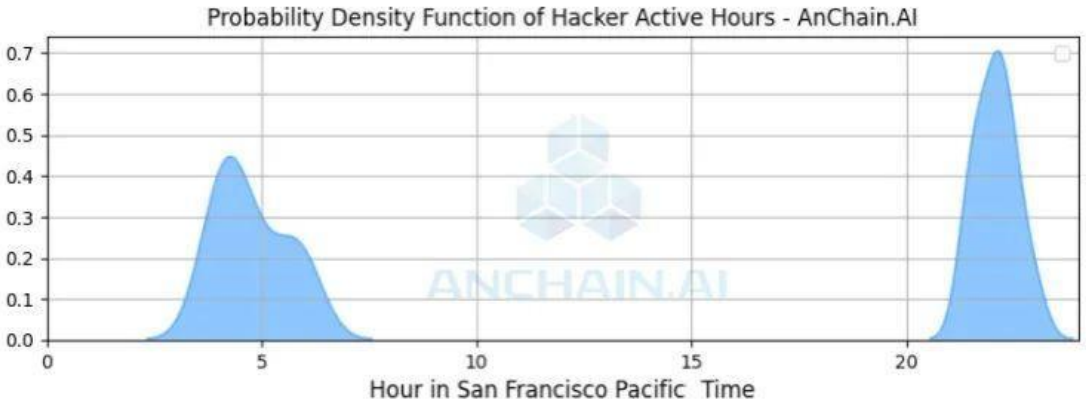

Figure: Hacker Active Hours

The probability distribution chart helps us figure out the best time to attack. If we start too early, there is a risk of spooking the criminals, and then our plan will go down the drain. In order not to attract the attention of the criminals, our best time is between 10am and 8pm EST.

Based on our assessment, this "Black Forest Demon" hacker appears to be a technologically savvy individual based in East Asia specializing in computer intrusion. However, they may have relatively limited familiarity with DeFi and smart contract technology.

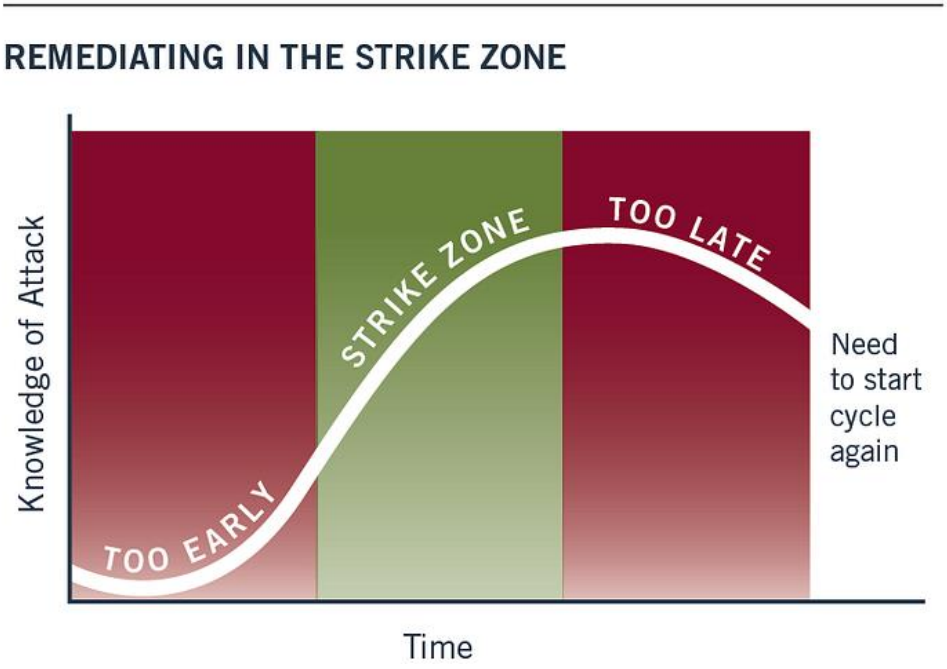

Figure: Mandiant's Incident Response Dictionary: Selecting the Time of Attack (Strike Zone).

Step 3: IR Program Development

The transaction mining belongs to the non-mainstream DeFi and thus the team conducted an in-depth analysis of its main smart contract source code overnight.

Plan A: Withdraw funds to a different wallet to avoid going through the victim's wallet

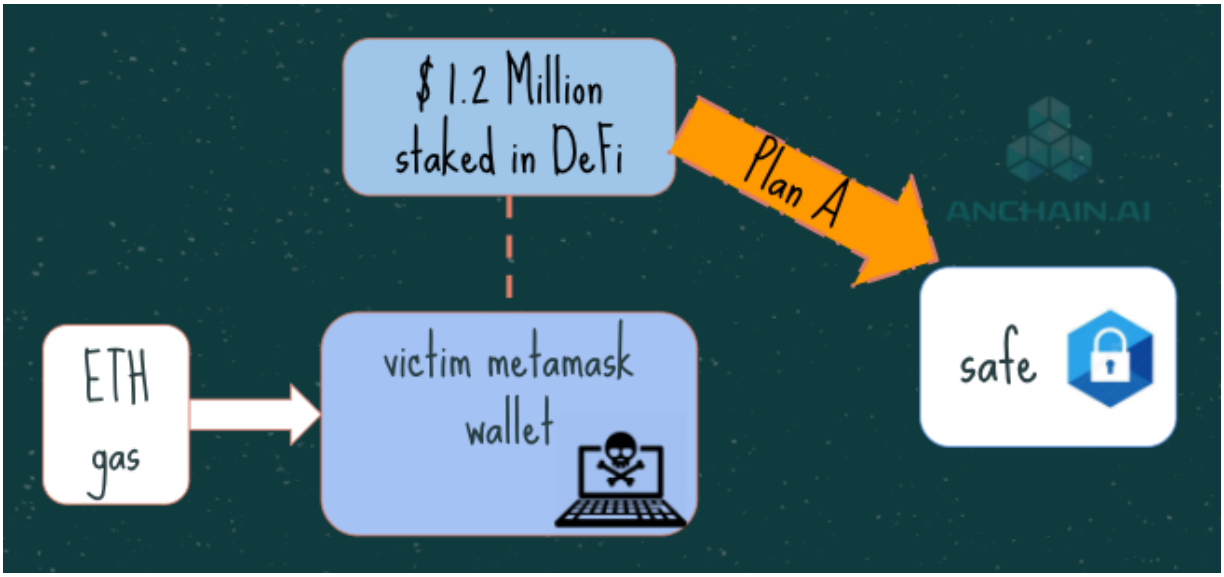

Figure: Withdraw funds to a different wallet

```
pool contract  @line
    function withdraw(uint256 amount) public updateReward(msg.sender) {
        require(amount > 0, "Cannot withdraw 0");
        if (breaker == false) {
            require(stakeLock[msg.sender] < block.number,"locked");
        }
        super.withdraw(amount);
        emit Withdrawn(msg.sender, amount);
    }
```

Figure: Code of withdraw function

Unfortunately, the withdraw() function does not define a receiver and can only withdraw assets to the original wallet. It is worth mentioning that Uniswap takes this situation into account and has set up procedures to deal with it.

Plan B: Can we freeze the assets? That way the hackers can't move the assets.

Asset freezing is a critical feature in DeFi governance.

```
token contract  @line :
    function _transfer(address sender, address recipient, uint amount) internal {
        require(sender != address(0), "ERC20: transfer from the zero address");
        require(recipient != address(0), "ERC20: transfer to the zero address");

        _balances[sender] = _balances[sender].sub(amount, "ERC20: transfer amount
        exceeds balance");
        _balances[recipient] = _balances[recipient].add(amount);
        emit Transfer(sender, recipient, amount);
    }
```

Figure: Code of transfer function

However, as you can see, there is no "lock" feature in trading for stablecoins.

Plan C: using the common "pause" admin function for emergencies in well-designed DeFi protocols.

However, upon reviewing this particular protocol, it appeared the "pause" function only suspended transactions at the token contract level, not personal wallet addresses. As such, it was deemed not suitable given the circumstances.

Regrettably, it seemed this product failed to sufficiently architect for potential enforcement scenarios like this.

Attempts were also made to contact the team through Telegram, email, tweets and their known partners/investors networks. However, a prompt response was not received, which can potentially stem from client support difficulties sometimes seen with DeFi products.

Plan Z: Surgery.

Plan Z is our last hope, and while it is fraught with risk, it can be concisely described through the following three steps:

- Transfer ETH to the stolen person's wallet as a fee;
- Withdraw pledged assets from the DeFi pool to the stolen wallet;
- All transferred to a safe place.

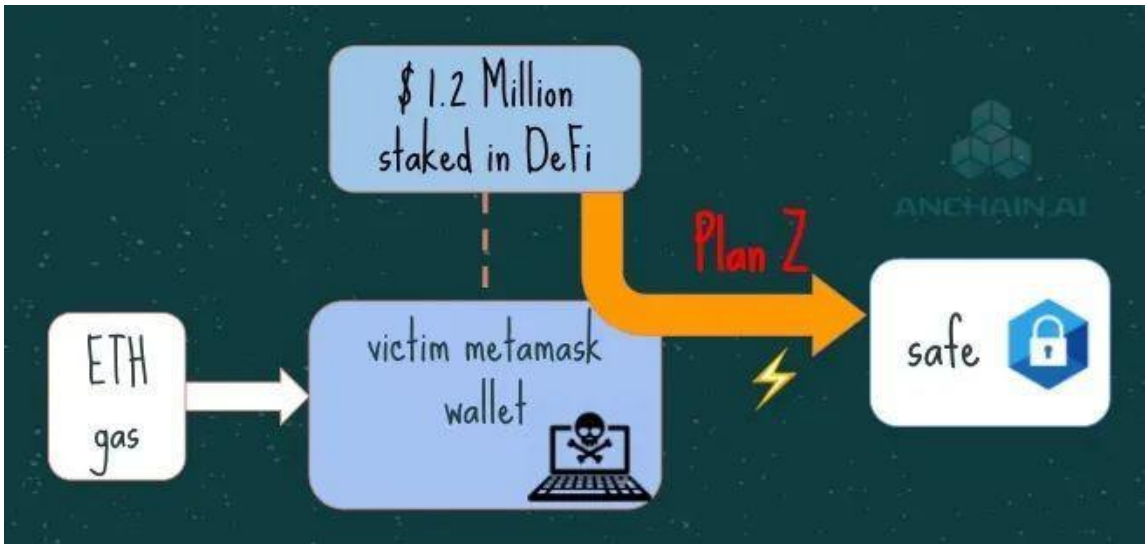

Figure: Plan Z: Surgery

We explained to the client the entire plan steps, game theory strategy, listing all scenario possibilities. The key to "Plan Z" is speed, and our automatic defense mechanism will increase our chances of winning.

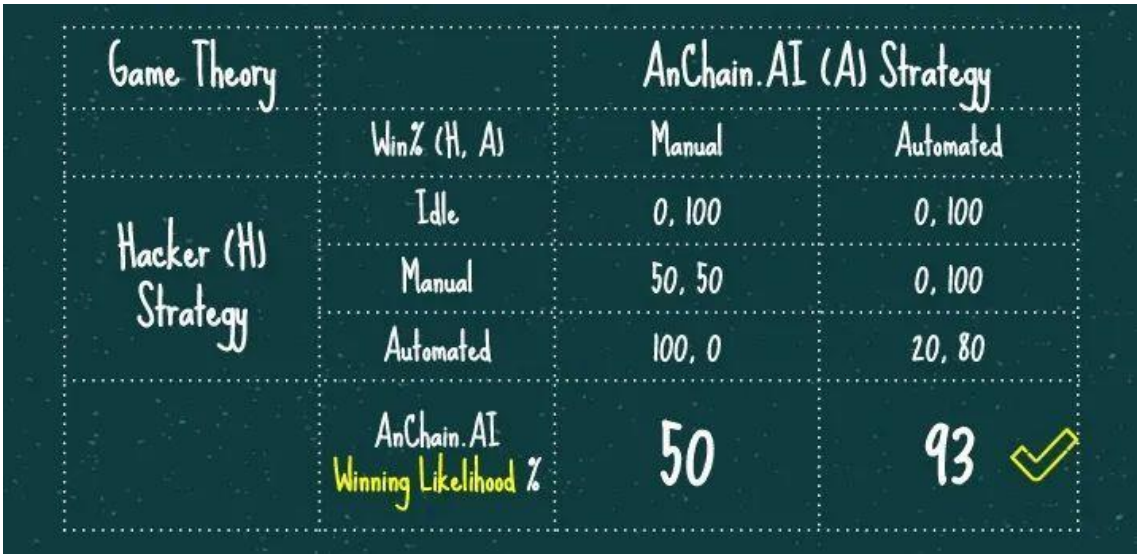

Figure: Plan Z: Game theory strategy

Even if the hacker uses an automated setup, our engineers have an 80% chance of winning the battle. Game theory shows that we have a 93% chance of winning this battle, which is promising. However, with so much money on the line, the potential 7% failure rate causes much stress and unease.

Plan Z is a blitzkrieg: our goal is to minimize the time lag between redemptions and transactions.

There are two crucial steps:

1) Redemption timeliness. Ensuring timely redemption by prioritizing transaction inclusion based on optimal gas fees. In 2020, during the booming period of DeFi, Ethereum faced significant network congestion and high fees, reaching a peak average gas cost of over 700 Gwei in June of that year.

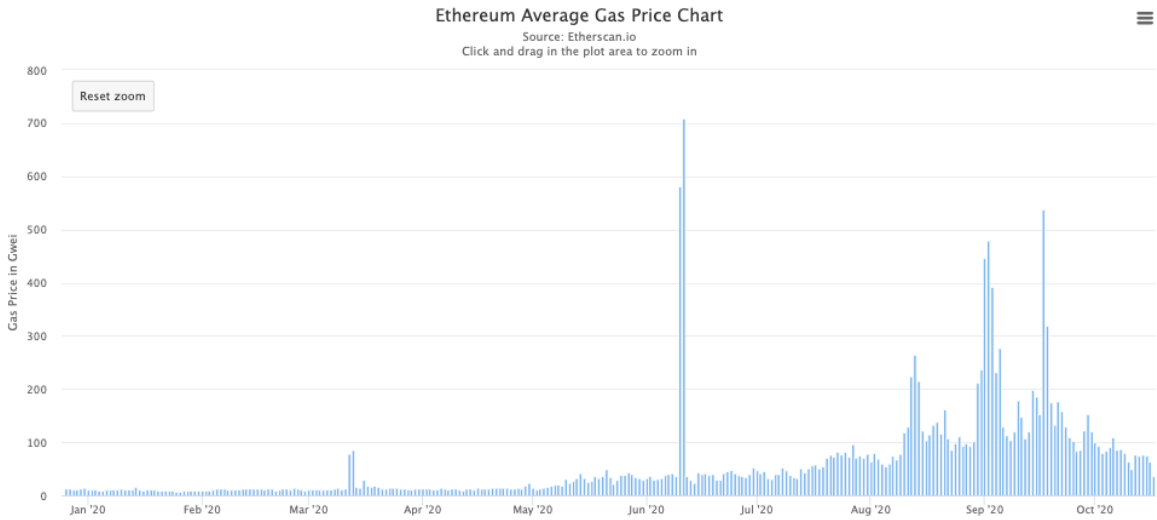

Figure: Ethereum Average Gas Price Chart

2) Within a mere 33 seconds of verification time, a fee of 200 Gwei has already become the top fee in the Ether pool for us. While any fee exceeding $12 to redeem a DeFi product may be considered very expensive, it becomes inconsequential when compared to a staggering amount of $1.2 million. Therefore, every second becomes crucial in such scenarios.

Step 4: Blitzkrieg

Our engineers quickly completed Python scripts that could Frontrun hacked transactions in the EtherMempool trading pool, ensuring that our ERC20 stablecoin transactions would be the first to be made in the DeFi pool and transferred to the safe place we had set up.

The offensive tool is now fully prepared, and we have named the file:

>> FrontrunDarkForest.py

We execute the Python script FrontrunDarkForest.py, which performs real-time monitoring of the Ether and proactively attacks.

The customer connects to the Metamask wallet, goes to the DeFi website, clicks on "Withdrawal" and confirms the 200 Gwei fee.

It was as if time stood still and all that could be heard was the sound of our heartbeats.

Thousands of Ether miners around the world in the SparkPool, Nanopool and F2Pool mining pools are desperately trying to get a piece of this deal.

After 30 seconds, the smart contract extraction transaction was successful, and the 200 Gwei transaction fee allowed us to steal away the hacker.

Soon, the script FrontrunDarkForest.py pops up with this message:

[INFO] Pre-transaction successful. USDC withdrawn to secure location.

After 3 seconds, the transaction is confirmed by the Ether Browser and the USDC arrives in the set secure wallet.

Technically, the incident response task was completed by 2:15 p.m. AnChain.AI rescued the $1.2 million Schrödinger's cat from DeFi's dark forest in 33 seconds. The world is still at peace, and the "demons of Asia" are apparently still dreaming, wondering if the hackers will wake up and regret it.

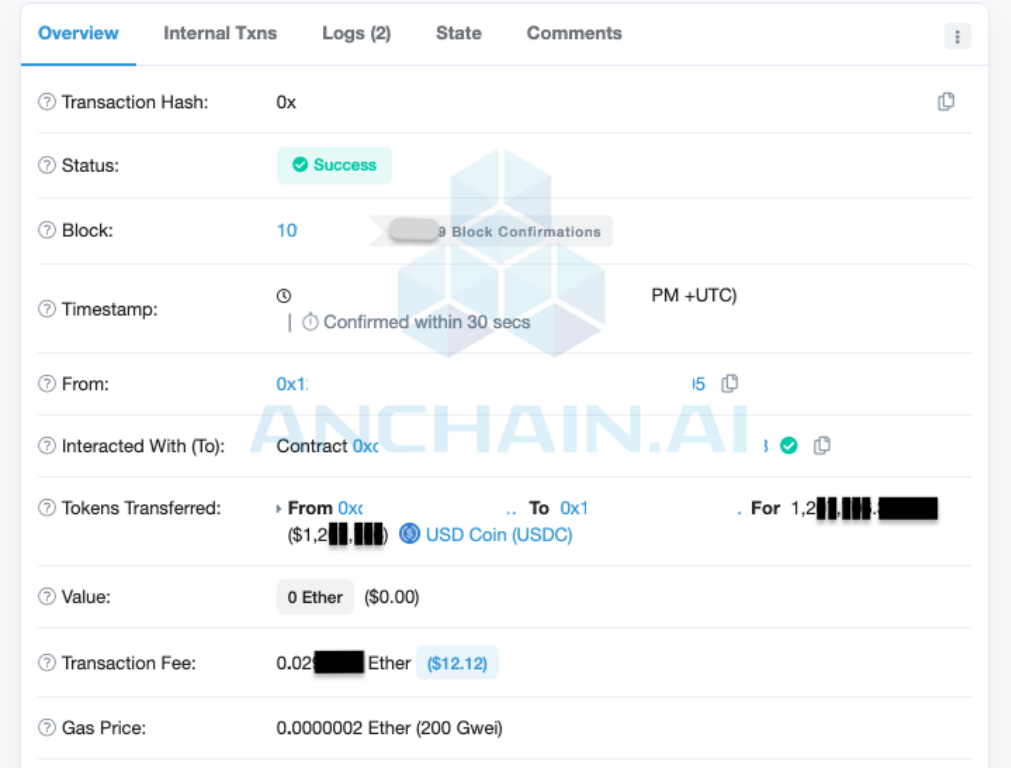

Figure: Transaction Chart

This success story highlights the technical strength of the AnChain.AI team and, more importantly, proves that the Web3 industry can successfully deal with hacker attacks.

Experience Sharing:

- Web3 Incident Response is a security program that must be highly valued by every digital asset team and must be planned from Day 1. (Note: The founding team of AnChain.AI is from Mandiant, a US-based company that was acquired by Google Cloud in 2022 and is an international leader in cybersecurity incident response). This example highlights 2 of the 5 key steps of the NIST Security Framework: Response and Recovery. For a systematic deployment of the Web3 Security Framework, see AnChain.AI's 2023 RSA Innovation Sandbox award-winning product Web3SOC [16]:
- Web3 blockchain incident response differs slightly from traditional computer security, rooted in the decentralized blockchain network and smart contract architecture.
    - DeFi smart contract analysis and business logic mining.
    - MEV and "robocall" analysis based on EVM blockchain Mempool memory pools.
    - Blockchain AML tracking and traceability, especially the challenging smart contract-based Tornado Cash, Uniswap and other new DeFi infrastructures.
- Web3 Hands-on skills for incident response programs:
    - Hacker Portrait: Hacker Attribution
    - Game Theory of incident Response Implementation Timing and Specific Implementation Options
    - Customer communication and cooperation

3.1.5.2.2.3 BLOCKSEC FIELD CASE - PARASPACE NFT LENDING PROTOCOL OPERATION RESCUE

On March 17, 2023, while monitoring transactions on the Ether chain, the BlockSec security team identified a suspected attacker address that deployed an attack contract. This contract attempted three consecutive attacks on the PareSpace NFT lending protocol from 3:51:23 UTC to 4:36:23 UTC. However, all three attacks were unsuccessful due to insufficient Gas Limit for executing these "complex" attacks. As a result, the pre-prepared funds allocated for the attacks were depleted, presenting a valuable opportunity for the BlockSec team to intervene and rescue the situation.

At 5:47:11, BlockSec's Rescue contract was successfully deployed, immediately launching a rescue "attack" on the hacker's premeditated target, the PareSpace contract, and successfully rescuing 2,906 ETH. The entire process was a race against time as BlockSec worked to locate the attack, coinciding with the upgrade of their monitoring system, Phalcon, which supports internal call analysis. Despite successfully identifying the attack, the excessive complexity of the hacked contract caused a data explosion, resulting in the collapse of the node and preventing automatic interception of the abnormal transaction, despite active monitoring. Thankfully, timely manual intervention, coupled with the attacker's mishandling of Gas, contributed to a favourable outcome.

This on-chain blocking behaviour helped ParaSpace to avoid a disastrous crisis event. This emergency action made BlockSec security team realize that even with a tight security monitoring system, some unexpected situations may occur in front of complex transactions, and a mature on-chain automatic blocking system has to be continuously upgraded and optimized through continuous on-chain blocking behaviour to improve the blocking success rate.

In fact, since BlockSec's automated monitoring tool Phalcon went live, it has helped a number of projects including Transit, FSWAP, Saddle, Platypus, etc. implement on-chain attack blocking, totalling $14 million in interception. In these successful cases, the BlockSec team uses a variety of attack blocking technologies, such as Frontrun, Counter Exploit, Automatic Contract Analysis and Auto-generation. Moreover, a reliable monitoring and blocking system should meet the characteristics of low false alarm rate and high coverage rate, and should detect potential attacks even when hackers deploy attack contracts to ensure sufficient time to respond.

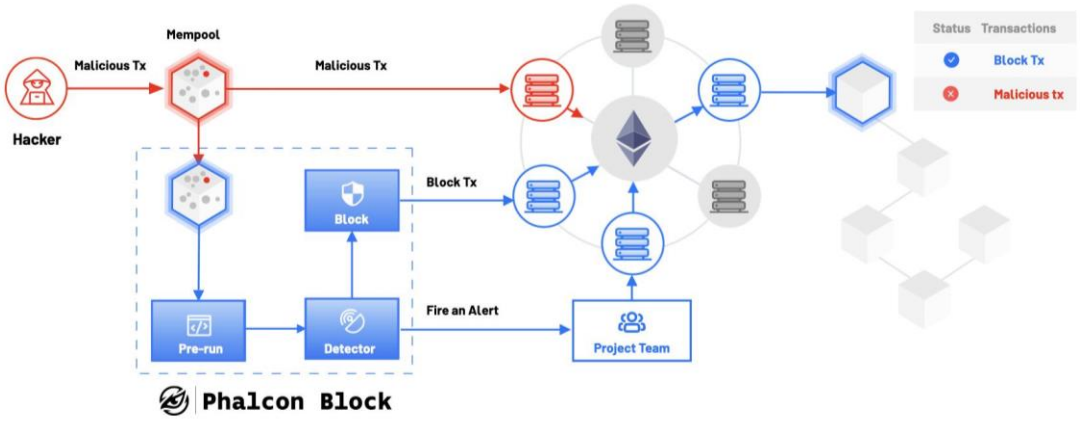

Figure: Phalcom Block

The reason why BlockSec team is able to "jump the gun" with hackers hiding in the shadows is that BlockSec has fulfilled the key link in the above web3 security practice: it has built a comprehensive on-chain behavioural monitoring and protection system, which listens to and collects transaction data of the whole chain, and detects and disposes of attack transactions. BlockSec's self-developed Phalcon system has been fully trained in the automated blocking process of listening, detection and disposal through a large amount of precipitated transaction data and many times of real-world interception experience. This experience is valuable for developers to reference during the product operation process.

3.1.5.2.2.4 SLOWMIST REAL-WORLD EXAMPLE - DEFI'S LARGEST EVER, POLYNETWORK CROSS-CHAIN BRIDGE ATTACK

On August 10, 2021, at 20:38, PolyNetwork was hacked, totalling over $610 million in crypto assets. Eventually, after 52 hours of tracking and negotiation, on August 12, the attackers returned $580 million in assets to Polynetwork.

After the attack, SlowMist team quickly contacted worldwide resources to draw the hacker's portrait and did vulnerability analysis, and united resources from all parties to do various chain possibility behaviour analysis. In the end, after two days of communication with the hacker, the stolen funds were returned.

The SlowMist team located the problem and found that its cross-chain contract Keeper had been modified to a hacker-specified address, allowing the hacker to arbitrarily construct transactions to remove any amount of money from the contract, specifically:

The main reason is that the Keeper of the EthCrossChainData contract can be modified by the EthCrossChainManager contract, and the verifyHeaderAndExecuteTx function of the EthCrossChainManager contract can execute the user's incoming data through the _ verifyHeaderAndExecuteTx function of the EthCrossChainManager contract can execute the data passed in by the user through the _ executeCrossChainTx function. Therefore, the attacker passes in carefully constructed data through this function to modify the address specified by the attacker for the Keeper of the EthCrossChainData contract.

SlowMist also found that the hacker prepared the attack of the first funds for the Monroe coins, and the Monroe coins will be recharged to the Tiger Exchange, exchanged for BNB, ETH, MATIC for the attack of the GAS fee. SlowMist then combined with the Tiger Rune to further investigate, and successfully located the attacker's mailbox, IP and equipment and other information. And when the hacker tried to clean the stolen money with Curve and other DeFi protocols, the transaction failed because the assets had been blacklisted by the exchange. During the process, Tether, the issuer of USDT, also played an active role by freezing the relevant illegal assets. This collaborative effort was aimed at intercepting as much liquidity as possible and preventing the hacker from successfully escaping with the seized funds.

Following the hacking attack, the process involved two key priorities. Firstly, efforts were made to intercept the hacker's funds to prevent money laundering and their escape. Secondly, a concerted effort was made to gather as many resources as possible to identify the hacker's identity. Subsequently, negotiations were initiated to secure the return of the stolen assets. Additionally, crucial clues were submitted to the judiciary, enabling the involvement of law enforcement agencies to assist in identifying and apprehending the suspects. Concurrently, intensive efforts were made to track down and block the stolen assets.

SlowMist's "Incident Response" practice in the PolyNetwork theft case fully applied its web3 security practice of asset tracking process workflow, including organizing the hacker's chain of asset transfer links, as well as other server snapshots, IPs, and other traces of hackers' profiles, etc. It is important to acknowledge that these systems have served as a "leverage" in deterring hackers from delaying the return of substantial amounts of stolen assets, even before involving law enforcement agencies. The effectiveness of these systems has acted as a "bargaining chip," facilitating the prompt recovery of significant stolen assets and helping mitigate losses within the crypto community.

The security team at SlowMist showcased professionalism and adherence to standardized practices throughout the asset damage tracking process. Their commitment to professionalism and standardization, along with the practical significance of their incident response practices in recovering lost assets, deserves commendation and serves as a valuable example for others to learn from.

3.1.5.2.2.5 ANKURA REAL-WORLD EXAMPLE - $120 MILLION CRYPTOCURRENCY PONZI SCHEME FRAUD CASE

Ankura was retained as a forensic investigator and consultant appointed by a large international Regulator, to investigate the recipients of a $120 million cryptocurrency Ponzi scheme fraud. Ankura has played a crucial role in assisting defrauded investors with the recovery of $30 million in total. This includes the recovery of various assets such as cryptocurrency, fiat currency, and investment assets. Ankura has successfully recovered cryptocurrency assets from centralized exchanges, DeFi smart contracts, and non-custodial wallets.

Ankura integrated a solution to access and analyse data from a variety of sources, including on-chain data as well as data from centralized and decentralized exchanges. Ankura team investigated over 30 cryptocurrency exchanges, over 200 exchange accounts, over 1,000 public keys, over 300 email accounts, over 90 Slack accounts, BOX enterprise accounts and AWS/Azure cloud accounts to find a complex network of assets including Bitcoin, ERC-20 tokens, DeFi, and NFT.

The team performed digital forensic analysis on computers, mobile devices, and other electronic devices to gather information to help recover stolen and misappropriated assets, including public and private keys for wallets and login credentials for exchange accounts. Ankura recovered public keys from a variety of information sources, such as browser history transaction logs, email communications, contracts with OTC providers, investors, exchanges, WhatsApp, Telegram, WeChat and Slack channels. Ankura also re-constructed private keys from non-custodial wallets in a variety of ways, including recovering passwords, cracking passwords, searching for seed phrases, searching for paper or hardware, and investigating transaction logs through subpoenas or injunctions issued by courts.

Multi-layer asset tracing was performed on both custodial and non-custodial wallets of interest, the team developed research memos and analysis to establish asset profiles to support efforts by the receiver to engage with entities and individuals who received stolen investor funds. In analysing public keys, Ankura utilized a variety of tools to drill down into public key balances, ERC 20 token balances, account transfer in/out records, links to known wallets, and revenue-generating tokens.

3.1.5.2.3 SUMMARY

The security solution for Web3 projects involves managing the entire lifecycle, from pre-development preparation to ongoing monitoring and establishing an incident response system. Adequate security considerations are essential to minimize the likelihood of security risks and prevent issues during project construction and operation. Developers need to cultivate security awareness and strictly implement necessary processes such as requirements analysis, code audits, unit testing, early warning and blocking procedures, and incident response mechanisms. By adopting these measures, developers can confidently navigate the complex security landscape of Web3 projects, ensuring a positive user experience and reliable service delivery.

3.2 SECURITY CHALLENGE II: CRYPTO BUSINESS PROFIT ATTRACTIVE, FRAUD RISKS, INDUSTRY GIANTS FELL

3.2.1 INDUSTRY PAIN POINTS AND SECURITY THREATS

The year 2022 was one of the most turbulent years for the digital asset industry, with the collapse of the Luna algorithmic stablecoin as the first big thunderbolt, triggering a series of chain reactions and laying the groundwork for the collapse of CeFi and capital institutions. There is no such thing as "too big to fail" in the digital asset field, even Three Arrows Capital, a native crypto capital institution that had been cultivating the industry for ten years and was one of the leading crypto capital institutions in the industry, also suffered from a major default due to its aggressive operating model and the fact that many of its assets went to zero due to the crash of Luna, causing it to use high leverage that caused the highly leveraged Three Arrows Capital to quickly collapse and became the first major crypto capital institution to file for bankruptcy in 2022. [17]

The collapse of the digital asset industry under the tidal wave of washing and scraping, a lot of poor management, lack of internal control, disregard for risk control and fraud and malpractice of the organization was also exposed to the surface, including Celsius, Voyager, FTX and BlockFi and other well-known giants which had fallen one after another. The bankruptcy announcement of FTX on November 11, 2022, came as shocking news in the digital asset industry in 2022. Its impact reverberated throughout the entire industry, leading to unforeseen consequences. Digital asset management organizations with limited risk resilience faced significant challenges and, in some cases, were compelled to declare bankruptcy due to liquidity issues stemming from the influence of FTX. Celsius improperly disclosed more than 14,000 pages of customer names, token types, net trade values, and deposit/withdrawal histories without regard to customer privacy, putting their privacy and even their lives at serious risk.

Through an analysis of the stormy bankruptcies of institutions like Three Arrows Capital, Celsius, Voyager, FTX, and BlockFi, it becomes evident that while the intermediate processes may vary, the outcomes are ultimately similar. The bankruptcy of institutions in the digital asset industry can almost always be attributed to capital greed, disorderly expansion, market turbulence, over-concentration of investment, insufficient liquidity, excessive risk exposure, fraud, misappropriation of client property, chaotic internal control management and inadequate risk

management mechanisms. In addition, there are highly complex affiliations within the digital asset industry, such as mutual lending, entity affiliations, mutual token holdings, etc., all of which can contribute to more serious runs and stampedes in the event of industry turmoil, further worsening and expanding the industry's pernicious effects.

The digital asset industry is gradually coming out of the haze since 2022, and major economies around the world, including the United States, the European Union, Japan, Singapore and Hong Kong, China, have been actively establishing a more transparent and reasonable regulatory framework for digital assets to deal with the rapid and disorderly development of the digital asset industry, so that the entire industry institutions and investors are fully protected. However, it takes some time for regulation to mature, and the self-discipline of the industry and enterprises is instead particularly important during this period. After experiencing rounds and rounds of baptism of wind and rain, investors will become more and more stringent in judging the good and bad of a digital asset management organization, and they will observe every move of the enterprise with a microscope, including technical capability, enterprise management capability, risk control capability, cybersecurity capability, and compliance conformity, etc., which has become an important evaluation index for investment decisions.

Digital trust is the cornerstone of the development of the digital asset industry, we should take the initiative to embrace regulation and rebuild investors' confidence in the industry under reasonable, transparent and clear rules. The reconstruction of the digital trust system should be done by "defeating magic with magic", building a trust system in the era of decentralization by means of cutting-edge cryptography technology, strengthening corporate internal control and risk management by means of the risk governance and internal control framework that has been verified by the traditional financial industry for a hundred years, and guaranteeing data compliance and the right to privacy by means of privacy science and technology. Once a digital trust relationship is established with investors, they gain the necessary confidence in the digital asset management organization. This, in turn, contributes to the overall prosperity of the industry.

3.2.2 STORYTELLING: BUILDING DIGITAL TRUST WITH USERS THROUGH ADVANCED TECHNOLOGY

The crypto industry takes four years as a cycle, and each cycle has a cycle of bull market and bear market, and the market fluctuates drastically, during which hackers also snipe closely at digital asset management organizations, delivering a fatal shot to the organizations that are already full of holes due to the market fluctuation. Therefore, digital asset management organizations that can traverse the cycle many times are bound to have the industry's top risk control and cybersecurity capabilities.

Amber Group, founded in 2017 by a team of finance professionals, has a long history of risk management in both traditional finance and digital asset markets. From the outset, Amber prioritized governance and developed a corporate governance system based on widely accepted frameworks such as the Committee of Sponsoring Organizations of the Treadway Commission (COSO) internal control and Control Objectives for Information and Related Technologies (COBIT) framework.

Over time, Amber has continually improved its technology, risk management, and compliance capabilities, obtaining various certifications from independent third-party auditing institutions such as SOC 2, ISO 27001, ISO 27701, ISO 29151, NIST Cyber Security Framework, NIST Privacy Framework, and PCI DSS. These certifications demonstrate Amber's compliance and security capabilities in protecting assets, networks, and data privacy.

Through years of investment and improvement, Amber has developed a tailored digital asset business security and robust risk management system, earning the trust of investors as a reliable digital finance service provider that can traverse industry cycles.

Amber Group has developed a digital asset business security and risk control system that leverages its years of expertise in compliance, internal control, risk management, and security. The system is designed to meet the unique needs of digital wealth management organizations, utilizing cutting-edge technology and advanced security measures. The system incorporates a full-stack custodial security framework supported by cutting-edge cryptography, ensuring robust protection of digital assets. Additionally, Amber Group has established a comprehensive digital asset business risk control framework and a data security and privacy protection framework to mitigate risks and safeguard users' information so as to rebuild trust amongst investors.

3.2.3 PRACTICAL CASES OF DIGITAL ASSET BUSINESS SECURITY AND RISK CONTROL SYSTEM

3.2.3.1 GENERAL

In the field of digital assets, cryptocurrencies are created, stored and circulated in the form of data, and the proof of ownership of cryptocurrencies is the private key, which will lead to a serious problem of financial loss once the wallet private key or confidential credentials are unauthorizedly accessed or leaked, so the security of confidential data and the security of funds are the key protection objects in the field of digital asset security.

Amber Group's digital asset business security and risk control system consists of a full-stack hosting security framework backed by MPC&HSM, a digital asset business risk control framework, and a data security and privacy protection framework that together form an *iron triangle*. By comprehensively identifying the risks of an organization's capital and data flows, it establishes multi-level technical and management controls to mitigate the impacts of fraud, malpractice and insider collusion and conspiracy, Misuse of Funds, Data Abuse, Data Misuse and Data Leakage risks, thereby rebuilding the industry's confidence in the digital asset space and enhancing users' digital trust in Amber Group.

3.2.3.2 DIGITAL ASSET BUSINESS RISK CONTROL FRAMEWORK

A digital asset management company should establish an enterprise risk management framework with the characteristics of its digital asset business. By identifying the industry's risk control standards and combining them with the company's business characteristics, the company should carry out comprehensive risk control management by means of an effective risk methodology for the risk domains of Counterparty Risk, Fraud Risk, AML & CFT risk, credit risk, market risk, liquidity risk, operational risk and internal control.

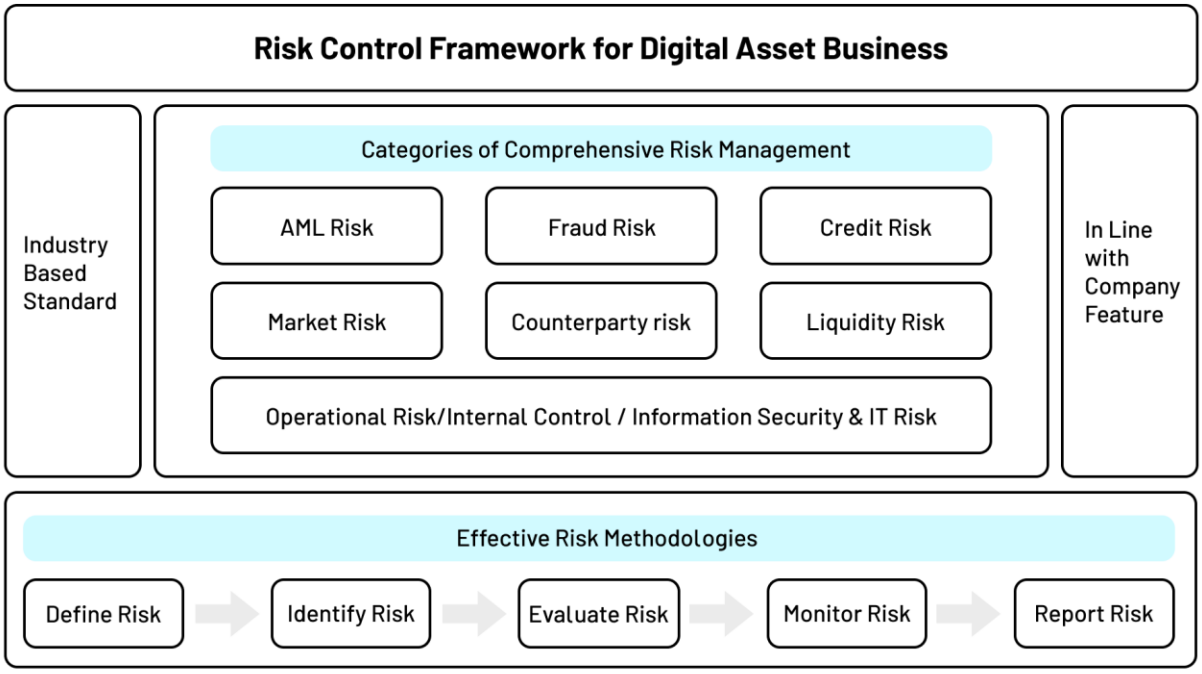

Figure: Digital Asset Business Risk Control Framework

Through the establishment of a comprehensive risk management organizational structure and the "three lines of defense" of risk management based on segregation of duties, the Company provides risk management with relevant functions such as coordination, decision-making, guidance, supervision and auditing, and can effectively provide the Board of Directors with risk analysis and decision-making support. In terms of risk management responsibilities, the responsibility of the "first line of defense" for business risk control should be strengthened, and a transaction operation team should be set up to strictly control business risks and continuously reduce potential internal control risks.

The business risk control framework for digital assets covers the following seven areas:

3.2.3.2.1 AML/CFT RISK MANAGEMENT

Money laundering and terrorist financing risks are the types of risks that crypto asset businesses need to be highly vigilant about. By taking advantage of the anonymous and decentralized transaction characteristics of crypto assets, money laundering is difficult to detect and the funds it transfers are difficult to trace. This not only seriously damages the credibility of the industry, but also encourages the growth of various types of illegal activities.

Digital asset management companies should cooperate extensively with regulators and other industry bodies to combat money-laundering. We utilize big data analysis and artificial intelligence to monitor the characteristics of customer transactions and the flow of funds, so as to detect suspicious money laundering and terrorist financing transactions in a timely manner and report them to the relevant authorities. We also regularly inspect business processes and technical systems to eliminate potential channels and means for money laundering and terrorist financing.

Strengthening the management of money laundering and terrorist financing is the unshirkable responsibility and obligation of digital asset management companies, which should be committed to creating a safe, high-quality and compliant business environment and combating any illegal and unethical behaviour. Only by ensuring that the platforms and tools for business operations are not utilized for illegal purposes can the long-term development value of the industry and assets be realized.

3.2.3.2.2 FRAUD RISK MANAGEMENT

Customer identity fraud is one of the most immediate risks to crypto asset businesses. At the business application and account opening stage, customers may submit fake identity information to conceal their true identity that cannot pass risk reviews. This may result in digital asset management companies being unable to accurately determine the risk level and attributes of their clients, facilitating illegal activities.

To prevent this risk, technical means such as artificial intelligence can be used to conduct comprehensive comparison and authenticity verification of customer identity information with application materials as well as IP, equipment and other information; at the same time, on-site body checking or video authentication can be conducted for certain customers on a random basis,

and their transaction characteristics can be continuously monitored during the course of the business in order to detect anomalies. Once customer identity fraud is detected, the relevant business will be immediately suspended and the customer relationship will be dealt with.

3.2.3.2.3 CREDIT RISK MANAGEMENT

Credit risk mainly targets the risk that the counterparty fails to fulfil repayment or fails to fulfil its contractual obligations on time, or adverse changes in the counterparty's credit standing, resulting in unanticipated losses to the Company. In order to comprehensively assess the credit risk status of customers, a credit risk scoring and measurement model based on customer registration information, transaction information and available external credit information has been constructed by applying industry's best practices to dynamically monitor and track the credit risk of each customer during the entire life cycle from registration, transaction to exit, ensuring that credit risk events are promptly identified and accurately assessed.

In order to improve the accuracy of the assessment, the segmentation analysis was conducted, and customers were divided into "professional investors" and "investment institutions". Separate credit scoring systems were established. The credit scoring model for "professional investors" covers demographic information, debt repayment history, credit history, number of new accounts, loan type and other dimensions. The credit scoring model for "investment institutions" covers financial information, basic information, industry information and risk warning. Based on the customer's overall credit rating and the overall risk control objectives, decisions are made on the customer's access, credit limit, pledge ratio, and pricing of the financing, among other strategies.

3.2.3.2.4 MARKET RISK MANAGEMENT

Market risk management is a process of mitigating losses by analysing market volatility, and monitoring and controlling risk exposures. It mainly involves risks in the cryptocurrency market, such as coin price fluctuations, exchange rate fluctuations, interest rate changes, etc., which may have a significant impact on an organization's financial position.

At this point, combining the traditional financial market risk management model and the trading characteristics of digital assets, market risk exposure is quantified and different risk exposures are set according to the trading strategy or investment objectives to ensure that the trading and investment teams minimize the market risk in line with the company's and client's risk appetite.

Common market risk indicators include Greeks (Delta, Vega, Gamma, etc.), Value-at-Risk, Leverage, Drawdown, Stop losses, etc. In the event that a risk indicator approaches or exceeds a predetermined limit, necessary actions are taken in accordance with market risk management policies and rules, including requesting the trading and investment teams to reduce positions and stop losses in a timely manner, and making necessary notifications and approvals to management.

In addition, based on the trading characteristics of digital assets and cryptocurrencies, additional monitoring of large asset movements on chain, large fluctuations in the price of cryptocurrencies,

and market sentiment analysis should be conducted to ensure that possible market fluctuations are recognized in advance and early warnings are issued to the trading and investment teams.

3.2.3.2.5 COUNTERPARTY RISK MANAGEMENT

Based on the characteristics of the crypto industry, it is necessary to define the counterparty risk mainly for the risk control of counterparties such as DeFi projects and centralized exchanges. Among them, for DeFi project, it mainly includes two aspects of code security review and business sustainability for assessment. The code security review mainly includes whether the code has been audited by a professional auditing company and whether the source code is consistent with the released code, etc.; the business sustainable development will focus on assessing the project's business model, potential profitability level, etc. The risk assessment of centralized exchanges is mainly based on their trading scale, transparency of reserves and platform registration information. Robust counterparty risk management will further implement differentiated concentration controls and set limits for counterparties based on their risk profiles.

Considering the industry characteristics of digital currencies, a comprehensive public opinion monitoring system can capture changes in counterparty risk status in real-time/quasi-real-time and help the firm dynamically adjust counterparty limit management. Based on business characteristics and data accessibility, the public opinion monitoring system can be constructed from negative public opinion, and platforms' token price fluctuations and net inflow and outflow of funds. When abnormal public opinion appears, the system will automatically notify risk management personnel for risk judgment and disposal.

3.2.3.2.6 LIQUIDITY RISK MANAGEMENT

The Company's liquidity risk is the risk that the Company will not be able to obtain sufficient funds in a timely manner or sell its assets at a reasonable price to pay its debts as they fall due, to meet other payment obligations and to satisfy the funding requirements for the normal conduct of its business. The monitoring indicators for liquidity risk are mainly divided into three categories: exposure indicators, non-exposure indicators, and liquidity risk monitoring indicators. Liquidity exposure refers to the difference between on- and off-balance sheet assets and liabilities maturing at different time periods in the future based on the contractual maturity date, obtained by subtracting the maturing assets from the maturing liabilities; when the difference is positive, it is called liquidity exposure; when the difference is negative, i.e., the maturing assets are smaller than the maturing liabilities, it is called liquidity gap. Non-exposure indicators contain leverage ratio and concentration, including asset concentration and liability concentration. Liquidity risk monitoring indicators encompass daily outflow forecasts, monitoring of liquidity coverage ratio indicators on a regular basis and under stress scenarios. In accordance with the prudential principle, the liquidity status of the counter assets (Coin Tier) is rated and high liquidity assets are screened based on the rating results, and the establishment of the above indicators and monitoring is based on high liquidity assets.

3.2.3.2.7 OPERATIONAL RISK AND INTERNAL CONTROL MANAGEMENT

3.2.3.2.7.1 OPERATIONAL RISKS AND INTERNAL CONTROLS FOR FUNDS TRANSFERS

Asset transfer operation, as an important segment in the asset security of digital assets, involves the change and handover of assets and carries certain operational risks. If the transfer operation is not standardized, it may lead to loss of assets, disputes over ownership, and operational errors.

In order to ensure the standardization and safety of asset transfer operations, the digital asset management company shall establish strict operating procedures and a monitoring mechanism. Asset transfer involves change of asset type, transfer of ownership, etc., which requires reclassification of assets, value assessment and accounting treatment in accordance with the regulations, as well as fulfilment of the necessary written agreement signing and approval process. Operators need to strictly follow the requirements of the procedures and keep detailed records of the conditions and operational details of the transfer, so as to leave traces of the operation and review it afterwards.

Asset transfer operations also require the handover and receipt of assets, and the handover personnel are required to confirm the quantity, status and change of ownership of the received assets, and immediately report and handle any abnormalities in the handover. We conduct regular inspections of asset transfer operations, focusing on the implementation of operational procedures, the completeness and accuracy of asset handover documents, and the timely updating of relevant system information. If operational irregularities or control loopholes are found, we will immediately review, rectify and pursue responsibility.

After a long period of standardized management, the operational risk of asset transfer can be effectively prevented and controlled. However, operational risk is characterized by the fact that it arises continuously with the changes in business and the increase in the number of execution links. At this point, it is necessary to further expand the depth and breadth of operation supervision, use security technology to monitor the whole process of operation, and organize regular drills to test the operation procedures and risk points. Operation standardization is the cornerstone of our continuous strengthening of asset management and risk control.

3.2.3.2.7.2 OPERATIONAL RISKS AND INTERNAL CONTROLS FOR INFORMATION SECURITY AND IT

Digital asset businesses need to emphasize ecosystem connectivity with institutions such as clients, exchanges (CEX & DEX), banks, custodians, and compliance service providers (KYC/AML/CFT/Travel Rule/Payment). If the management model and specifications of key elements of the ecosystem interconnections such as account numbers, permissions, APIs, CAPTCHAs, and business rules are inconsistent, it can lead to significant impacts on digital asset management organizations in the areas of internal control, risk control, security, and finances. These may include account misuse, loss of API control, data leakage, financial loss, internal

collusion, misappropriation of funds, inconsistent financial reconciliations, and complicity in key business processes, among other serious implications.

The security and risk control framework of digital asset businesses are established to solve these problems. After polishing and optimizing the technology, process, and mechanism for an extended period, a comprehensive and effective risk control means based on AI, with the characteristics of the digital asset field, has formed. This helps to win the trust of high-net-worth clients and institutional clients.

Exchange Account Permission and API Control Security

To have electronic market making, quantitative trading, and trade execution services, digital asset management institutions need to connect with multiple centralized exchanges (CEX) and place orders to execute trades. Each CEX has unique account and authority management specifications, usually divided into master and sub-accounts, and permissions for high-risk operations such as withdrawal of funds, deposits, digital wallet address whitelisting, money transfers, exchanges, and trades. Permissions have different permission level definitions, and the APIs created for relevant accounts will also differ in terms of trading operation permissions such as leverage, options, and intra-account transfers.

To ensure unified management and authorization accuracy and consistency across N exchanges for X accounts and Y permissions, digital asset management organizations need a well-developed CEX account permission management platform and supporting policies and processes. They should establish an internal account management system and transaction control system that can effectively deal with large-scale account authority management issues, enhance account interoperability and scalability in the upstream and downstream of the digital asset ecosystem, and put an end to high-risk issues such as account mixing, sharing, and abuse.

- Internal Account Management System: Realize the unified management of CEX account privileges in the whole life cycle of application, creation, entry, authorization, sharing and deletion, and establish the effective separation of the three lines of defense of operation, management and auditing through the effective internal control mechanism of separation of duties, including the separation of application and approval, the separation of entry and use, and the separation of management and auditing;
- Transaction Control System: Enables secure management of API trading privileges under the CEX account, providing individual authorizations for each combination of API trading operations based on the principles of minimization and need-to-know, with each API authorization tied to a specific user and automated trading program. The transaction control system also enables wallet creation, smart contract creation and authorization for decentralized exchanges (DEX), setting up a whitelist of outgoing wallet addresses, as well as monitoring funds to meet the security needs of DeFi trading. The system has perfect pre-authorization, monitoring and auditing capabilities, and can provide strong control over key trading operations.

A. AI-BASED BUSINESS-CRITICAL CONTROL OF DIGITAL ASSETS

The key operations of digital asset management are generally related to the flow of funds and the flow of confidential data, and any operation involving the loss of funds and the leakage of confidential data requires the establishment of prudent approval and control mechanisms.

Through the business security risk assessment method based on data and capital flow, the risk of business scenarios involving loss of funds and leakage of confidential data is identified, analysed and evaluated, in which key control processes are constructed for high-risk risks, including authorization and approval, retention of transaction credentials, grading and control of the transaction amount, etc., and with the separation of duties in the key processes, job rotation, mandatory vacations, monitoring of key positions and independent auditing and other safeguard mechanisms can effectively prevent internal fraud and malpractice risks. With the key processes of segregation of duties, job rotation, mandatory vacation, monitoring of key positions and independent auditing and other safeguard mechanisms, the risk of internal fraud can be effectively prevented.

Through AI technology, it can quickly extract the customer's quote information in the trading chat room, and automatically summarize and abstract the information, summarize and analyse the information through AI, and form the trading order and trading evidence automatically retained, which greatly improves the efficiency, timeliness and compliance of the transaction.

Amber Group has been at the forefront of leveraging LLM-based artificial intelligence (AI) technology and chatbots to enhance business support capabilities. They are pioneers in applying these innovative technologies in various areas, such as quote information summarization, analysis, and automated retention of trading evidence for trading orders.

This creative approach demonstrates their commitment to utilizing cutting-edge technologies for the benefit of their clients and the industry as a whole. By leveraging AI and chatbots, Amber Group has streamlined business processes, improved efficiency, and enhanced the overall user experience.

B. DATA SECURITY ISOLATION SANDBOX OPERATING TERMINAL

The data security isolation sandbox operation terminal is specially designed for personnel who need to interact with CEX on a daily basis, and it is managed by the privileged account management system (PAM). The sandbox is isolated from workplace office computers, which can eliminate malicious viruses and Trojan horse attacks, and also ensure data security isolation, while providing perfect operation auditing capabilities to establish a credible and controllable secure transaction environment.

C. HOSTING AND SHARING OF PASSWORDS AND CREDENTIALS

In the process of interconnecting with various ecological organizations, digital asset management organizations will inevitably have passwords, credentials, access keys and secret keys that need to be securely stored, used and shared to ensure the security of confidential data. The password and credential management platform built by cryptography mechanism can provide security protection for the whole life cycle of password and credential entry, storage, distribution, authorization, use, update, sharing and destruction, ensuring that only authorized users can use corresponding passwords and credentials in necessary business scenarios, and that users can't know the specific explicit passwords and credentials, so as to achieve the goal of "available but not visible" password and credentials. The data protection effect of "available but not visible" is achieved.

D. EXCHANGE CAPTCHA AUTHORIZATION PLATFORM

Service providers in the digital asset ecosystem (e.g., CEX) all set up multi-factor authentication (MFA) in key business processes to challenge and validate user requests twice, and the validation methods are usually email CAPTCHA and SMS CAPTCHA. Digital asset management organizations usually create public accounts with service providers, but public accounts need to be bound to email or cell phone numbers to receive verification codes. Binding an employee's personal email or cell phone number may result in CEX's key operational processes being completed by a single employee on his or her own, which poses a greater operational risk.

The digital asset management company should build an exchange verification code authorization platform to receive the verification code from CEX through a dedicated enterprise mailbox and enterprise phone, and match it with the approval process of key business control of digital assets, and distribute the verification code to the applicant only when the approval process matches the verification code successfully to realize the precise mapping of "person-process-verification code" and "person-process-verification code". Accurate mapping is achieved, which greatly enhances the effectiveness of key business control and transparency of key operations.

E. REAL-TIME SECURITY RISK CONTROL DECISION PLATFORM

Building a real-time business risk control decision-making platform gives a comprehensive but unique multi-dimensional view to minimize or eliminate potential risks including account theft, transaction fraud, security attacks and more.

The core underlying data framework of real-time risk control system is established by collecting data such as equipment information, network information, and operation behaviour during the business process. In addition, the third-party black and gray industry data, AML, KYC data assistance, to enhance the richness of the data. On this basis, different threat models are established based on different scenarios, and then differentiated strategy sets are created for the threat models. Match the risks in the business data flow through the real-time policy engine. At the same time, risks and corresponding decision-making processes are visualized through work orders, reports, and graphics in a way that not only helps in pre- and post-defense, but also thrives on the damage associated with internal and external data resources.

By now, most emerging and even traditional business scenarios such as anti-money laundering (AML), travel rules, account security, know your transaction (KYT) and know your customer (KYC) are fully protected. Meanwhile, with the internal decision engine and powerful computing capabilities, high-quality decisions at the millisecond level have been realized across business lines.

3.2.3.3 MPC & HSM-ENABLED FULL-STACK CUSTODY SECURITY FRAMEWORKS

Amber Group has adopted industry-leading digital asset custody solutions and introduced more advanced technologies and security measures. Through leveraging both cold and hot wallet technologies such as multi-signature wallets, multi-party computation (MPC) and HSM, the integrated solution meets regulatory requirements in functionality, compliance and security, this ensures the digital asset custody solution meets the highest security standards.

3.2.3.3.1 ADOPTION OF TECHNOLOGY - HSM (HARDWARE SECURITY MODULE)

In the context of technology adoption, the utilization of Hardware Security Modules (HSM) is crucial for ensuring the security of custody infrastructure. RigSec Technology Limited's financial institution grade custody infrastructure serves as an excellent example in this regard. This comprehensive all in one custody solution integrates various elements, such as Hardware Security Modules (HSM), personal security devices (PSD), and a robust software service system. By leveraging these components, the infrastructure effectively safeguards transaction private key information and risk control strategy information, thereby ensuring the security of the entire digital asset storage and transaction process. Additionally, this solution is specifically designed to meet compliance requirements established by regulators in regions like Hong Kong, Japan, and Singapore. RigSec Technology Limited's custody infrastructure is built with a strong emphasis on security and compliance, providing a reliable and trustworthy solution for digital asset management.

3.2.3.3.2 OVERALL HSM SOLUTION ARCHITECTURE

Digital asset custody is a technical solution combining software and hardware. The main components of the solution include:

1) **HSM (hardware security module) hardware**: Used for generating digital asset root seed, private keys, key generation, storage and transaction signing for cold and hot wallets. It is recommended that the HSM should meet NIST FIPS140-3 CMVP level 3 certification requirements;

2) PSD (personal security device) hardware: For wallet administrator, operator authentication, management configuration and transaction approval. It is recommended that the security chip should meet CC EAL4+ security level and pass FIPS140-2 CAVP certification;
3) Wallet software systems: Including wallet management system and wallet business system, for administrators to manage configuration policies, and wallet operators to approve transfers etc;
4) Cold wallet offline Air-gaped Vault system.

3.2.3.3.3 KEY FEATURES OF RIGSEC'S COMPLIANT CUSTODY SOLUTION

1. END-TO-END VISIBILITY AND SIGNING THROUGH PSD DEVICES

Withdrawal operations require approvers to confirm detailed information on the PSD device, which then digitally signs the key data (token currency, target address, amount, etc.). The HSM only uses the private key for transaction signing after verifying the PSD signature. This ensures the integrity of key data in the on-chain transaction matches what was seen and signed on the PSD, preventing man-in-the-middle attacks.

2. ENFORCED RISK CONTROLS THROUGH SECURE HARDWARE

Admins have the ability to define customizable risk policies within the Hardware Security Module (HSM). These policies undergo mandatory checks prior to signing transactions. The checks include:

- Multi-level authorization based on the transaction amount;
- Whitelisting of approved addresses;
- Daily cumulative approval limit to manage transaction volume;
- Maximum Gas Limit to prevent misuse and errors.

3. INSTITUTIONAL-GRADE ROLE-BASED ACCESS MANAGEMENT

- Complete separation of roles and responsibilities;
- No single user can move funds or make changes independently;
- Transaction authorization via trusted hardware PSD.

4. HIGH STANDARD OF SECURITY CERTIFICATIONS

- Random numbers generator meets NIST SP 800-90B entropy source standard;
- Security chip is certified under FIPS 140-2 Cryptographic Algorithm Validation Program (CAVP);
- HSM Security Hardware Module meets FIPS 140-3 Level 3.

5 HIGH AVAILABILITY AND ROBUSTNESS

- One-stop deployment for cold and hot wallets;
- API access and user-friendly software UI;
- Supports cluster deployment to achieve high availability and robustness of the system.

6. MEETING COMPLIANCE SUPPORT

- Integrated AML services to meet regulatory requirements;
- Comprehensive reporting and logging capabilities enable for financial reconciliation and auditing;
- Multi-factor user authentication mechanism;
- high security standard.

7 MULTI-PUBLIC CHAIN SUPPORT

Supports more than 30 mainstream public chains, and can flexibly support the addition of tokens on public chains as configured by customers.

3.2.3.3.4 PRIVATE KEY SECURITY

Private key security is an important component of digital asset custody solutions, mature custody solutions have clear specifications and division of responsibilities in terms of private key lifecycle security, private key co-management security, multi-party asset custody, prevention of single-point risk and private key usage security, the main roles of the program include:

- Root Seed Piece Holder: Responsible for the safekeeping of HSM Root Seed Pieces or restoring HSM Root Seed as needed. Performed by company partners or executives.
- Administrator: Responsible for configuration management of the wallet system, such as setting up transfer approval policies, setting up whitelists, etc. Performed by enterprise management personnel;
- Operator: Responsible for withdrawals or transfers approvals, etc., by the wallet system operator or finance staff;
- Others: Such as auditors, compliance, observers, etc.

3.2.3.3.5 MNEMONIC PHRASE MANAGEMENT

The HSM wallet implements multi-party co-management of assets and prevention of single points of failure by splitting the root private key into multiple fragments using Shamir's Secret Sharing algorithm. These fragments are independently held by multiple individuals. Retrieving the root private key requires participation from multiple individuals. The root private key fragments are generated and recorded onto titanium plates by designated mnemonic administrators, they are then securely stored. The process of private key usage involves mandatory review and enforcement of business workflows and transaction strategies.

3.2.3.3.6 PRIVATE KEY MANAGEMENT

Blockchain uses asymmetric cryptography to manage assets on-chain. where assets are locked to a public key or address associated with the public key. Asset managers utilize corresponding private keys to control the assets. Strict internal policies and procedures are established and enforced for private key management to ensure secure seed generation and storage of all encrypted seeds and private keys.

1. ROOT SEED PRODUCTION

Seed and private keys are generated according to applicable international security standards and industry best practices, ensuring the wallet seeds or private keys are produced via non-deterministic methods with verifiable randomness, and cannot be reproduced.

2. ROOT SEED STORAGE

After the root seed is generated, it is stored in a secure chip that can only be used for computation and cannot be exported.

3.2.3.3.7 SOURCES OF RANDOMNESS

Cryptocurrency security standards also provide a number of security requirements for the private key generation process of cryptocurrencies, including the use of high-quality random number generators and physical sources of randomness to ensure the randomness of the seed phrases. This improves the security of cryptocurrencies and prevents the private key from being maliciously obtained or guessed. By utilizing a physical random noise source as the source of the seed and complying with the relevant standard requirements, the cryptograph is able to ensure the randomness of the seed, which enhances the security and strength of the generated key and encryption algorithm.

The device's source of randomness for seeds is physical random noise sources. The design should comply with the standard specifications of NIST SP800-90B.

3.2.3.3.8 TRANSACTION AUTHORIZATION STRATEGY

A Transaction Authorization Policy (TAP) is a set of rules that governs the limits and conditions for fund transfers. It enables control over which user roles can initiate fund transfers, sets limits on transaction amounts (both per transaction and daily limits), and determines the approval process for transactions. Wallet services employ various transaction authorization mechanisms, including:

- Multi-person, multi-level approval mechanism;
- Mechanism for whitelisting addresses; mechanism for limiting the total amount of transactions;
- Transaction fee limitation mechanism;
- Transaction authorization policies for wallet services are set and approved by the administrator role.

3.2.3.3.9 ROLE-BASED MULTIPLE AUTHORIZATION SCHEME

The digital asset custody solution uses a top-down hierarchical authorization mechanism to ensure that the governance process is safe and reasonable and to reduce the risk of a single person committing an evil act, in addition to the transaction can only be initialized by the customer, the main measures are:

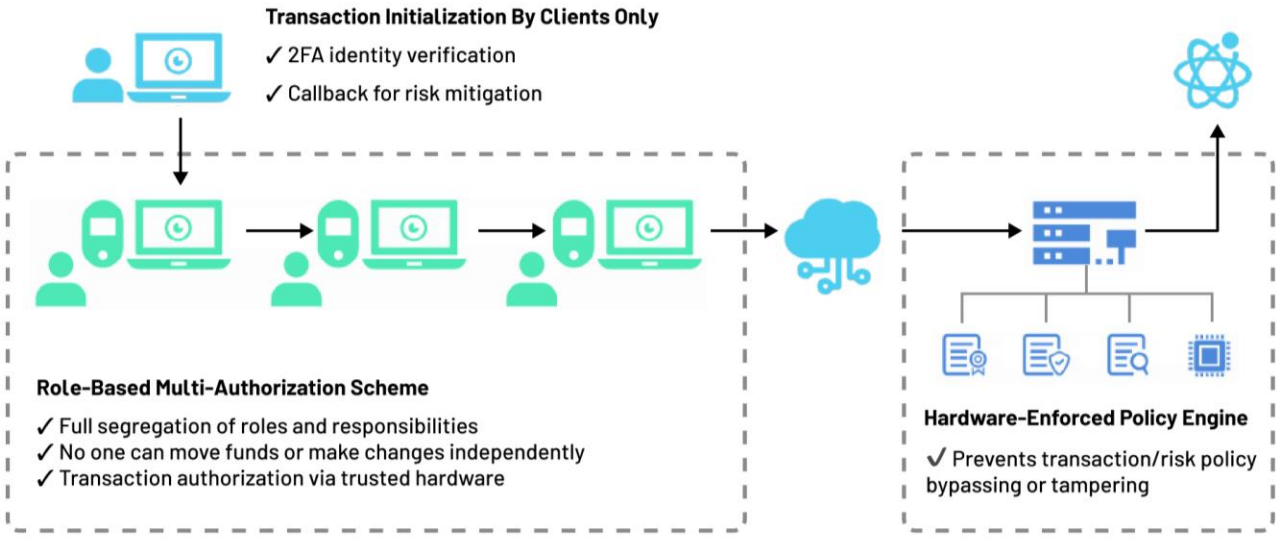

Figure: Role-based multiple authorization scheme

Transactions can only be initialized by the customer

- Two-factor authentication;
- Fallback mechanisms for risk mitigation;

Role-based Multiple Authorization Scheme

- Complete separation of roles and responsibilities;
- No one can move funds or make changes independently;
- Transaction authorization via trusted hardware;

Hardware-enforced Policy Engine

- Prevent trading/risk strategies from being bypassed or tampered with.

3.2.3.3.10 PHYSICAL SECURITY OF ENCRYPTION MACHINES

To ensure the physical security of the encryption machine equipment, a variety of measures, including security controls, environmental monitoring, and physical security measures, should be taken to protect it from threats such as unauthorized access, destruction, tampering, or theft.

3.2.3.3.11 NETWORK SECURITY

To ensure the robustness and proper maintenance of all systems and processes within the Wallet System, and to minimize and manage risks such as theft, fraud and other dishonest acts, professional misconduct, errors and omissions, service interruptions, or other operational or monitoring deficiencies, key security controls are implemented. Some of these controls include, but are not limited to:

1) The wallet system, involving fund transactions, is considered a core system, and its security controls should align with the enterprise's internal core systems.
2) Implementing appropriate network isolation to protect the wallet system within a segregated network segment. Only necessary ports and services should be accessible, and any network changes must follow the standard enterprise change management process, including review, testing, and approval before implementation in the production environment.
3) The backend servers, cloud infrastructure, and databases supporting the wallet system should adhere to the standard configuration baseline established by the firm. Critical configurations like high-risk port services, privileged server accounts, and audit logs should meet industry security standards. Regular baseline scanning should be conducted to identify potential non-compliant items and address them promptly.
4) Regular penetration testing and vulnerability scanning should be performed on wallet system services to identify and remediate security vulnerabilities in a timely manner.
5) Authorization of privileges for wallet system services should follow the "principle of least privilege." Privileges should be aligned with users' job duties, avoiding excessive granting of privileges. Regular reviews of account privileges should be conducted, and unsuitable privileges should be promptly changed and managed.
6) Collecting application logs and infrastructure-level audit logs from the wallet system and integrating them into the enterprise's security operation system. This enables real-time monitoring and response to security incidents and events, particularly for high-risk scenarios such as unauthorized logins, abnormal IPs, and unusual fund transactions.

3.2.3.3.12 ADOPTION OF TECHNOLOGY - MPC (SECURE MULTI-PARTY COMPUTATION)

Secure multi-party computation (MPC) enables multiple participants who do not trust each other to compute any function correctly while keeping the input and output information of each party private. In simple terms, multiple parties have their own private data, but can collaborate to compute the result of an objective function on each party's private data without disclosing their own private data. The entire computation is done without any knowledge of each other's private data.

Securing the storage and movement of cryptocurrencies is key to expanding a company's business, which can be further enhanced with a multi-party computing (MPC) technology infrastructure. Utilizing Multi-Party Computing (MPC) technology solutions not only focuses on high-speed transactions, but also ensures that security is not threatened technology solutions provide a secure infrastructure for moving, storing, and distributing digital assets, which can be effectively protected through MPC technology and chip-level hardware isolation. This innovative approach protects the customer's private keys, making API keys and deposit addresses from cyber-attacks and internal fraud, while MPC-based key management services eliminate single points of failure. With the solution's secure transport environment, customers' digital assets are protected from movement across exchanges, custodians, over-the-counter brokers, hot wallets and cold storage. Additionally, for risk prevention reasons, the solution provides end-to-end insurance for assets stored and in transit.

3.2.3.3.13 INTRODUCTION TO MPC WALLET SECURITY MECHANISMS

Amber Group has formed a strategic partnership with a top-tier MPC (Multi-Party Computation) wallet provider to enhance the security of its clients' digital assets. The MPC service provider contributes the core technology and wallet platform, ensuring the protection of clients' assets. Amber Group, on the other hand, takes charge of transaction operations, authorization, and monitoring, ensuring seamless and secure asset management for its clients. This partnership combines the expertise of both entities to deliver robust security measures for the protection of digital assets.

Private keys are generated and protected by the MPC service provider, and wallet key creation and signing are protected by multiple components and mechanisms, including secure multi-party computation, chip-level hardware isolation, and a transfer-amount-based policy engine, whose security is based on a multiple-defense approach in which wallet key creation and signing are protected by multiple, complementary approaches:

- Secure Multi-Party Computing (MPC): Private keys are never stored centrally in one place. Creation, signing, and revocation operations take place in a distributed, untrusted manner across multiple co-signing components;
- Chip-level hardware isolation: all key material is protected in a hardware-isolated environment. In addition, any code or data that could be a threat is executed in a hardware-isolated environment;
- Policy Engine: Transfer amount-based restriction policies are enforced by any of the co-signing components to ensure that attacks on either the originating customer, or the centralized component between the customer and the co-signer, are blocked. The policy engine allows the user to configure a set of rules that affect how transactions are processed and approved. Rules can set whether transactions are blocked, approved or require additional signers, using filters such as source, target, asset and amount.

3.2.3.3.14 TRANSACTION AUTHORIZATION POLICY

Strict transaction authorization policy should be established, segregating different users into different groups. Approval authorization is done based on groups, roles, and amounts. Using a transaction authorization policy, it is possible to control which user roles can transfer funds, how much funds can be transferred in a single transaction or per day, and how to approve transactions; there are the following transaction authorization mechanisms for wallet services: multilevel approval mechanism, whitelisted address mechanism, transaction amount limitation mechanism, transaction rate limitation mechanism, and transaction fee limitation mechanism. the transaction authorization policy ensures that the governance process is secure and reasonable. Reducing the risk of single-player mischief.

3.2.3.3.15 KEY BACKUP AND RECOVERY

Digital asset management companies should have backup and recovery controls in place to ensure that customers always have access to assets, even in extreme cases where they lose access to all their key shares or the MPC vendor suspends operations. Backup functionality needs to be set up in a configuration item on the MPC service provider to ensure sufficient flexibility in backup and recovery operations.

3.2.3.3.16 INDEPENDENT AUDITS

The MPC service provider is recommended to pass a SOC2 Type II audit attestation to demonstrate its security, availability, and confidentiality in compliance with the control principles set forth in the AICPA standards, and after a rigorous, independent audit process, no deficiencies were identified in the course of which the service was audited.

3.2.3.4 DATA SECURITY AND PRIVACY PROTECTION FRAMEWORK

3.2.3.4.1 INTRODUCTION TO DATA SECURITY AND PRIVACY PROTECTION FRAMEWORKS

The Data Security and Privacy Protection Framework is an important link that forms the iron triangle of the digital asset business security and risk control system, with the main purpose of preventing data abuse, data misuse, data leakage and privacy compliance risks within the organization. The Data Security and Privacy Protection Framework is based on the NIST Privacy Framework, incorporating the Data Security Capability Maturity Model requirements (DSMM), SOC 2, and the ISO Information Security and Privacy Information Management System (ISO 27001/27701/ 29151), and combining Privacy by Design and advanced cloud-native Combined with Privacy by Design and advanced cloud-native DLP capabilities, this comprehensive framework for digital asset data privacy protection lays the foundation for Amber Group to build digital trust and enhance privacy transparency with its clients.

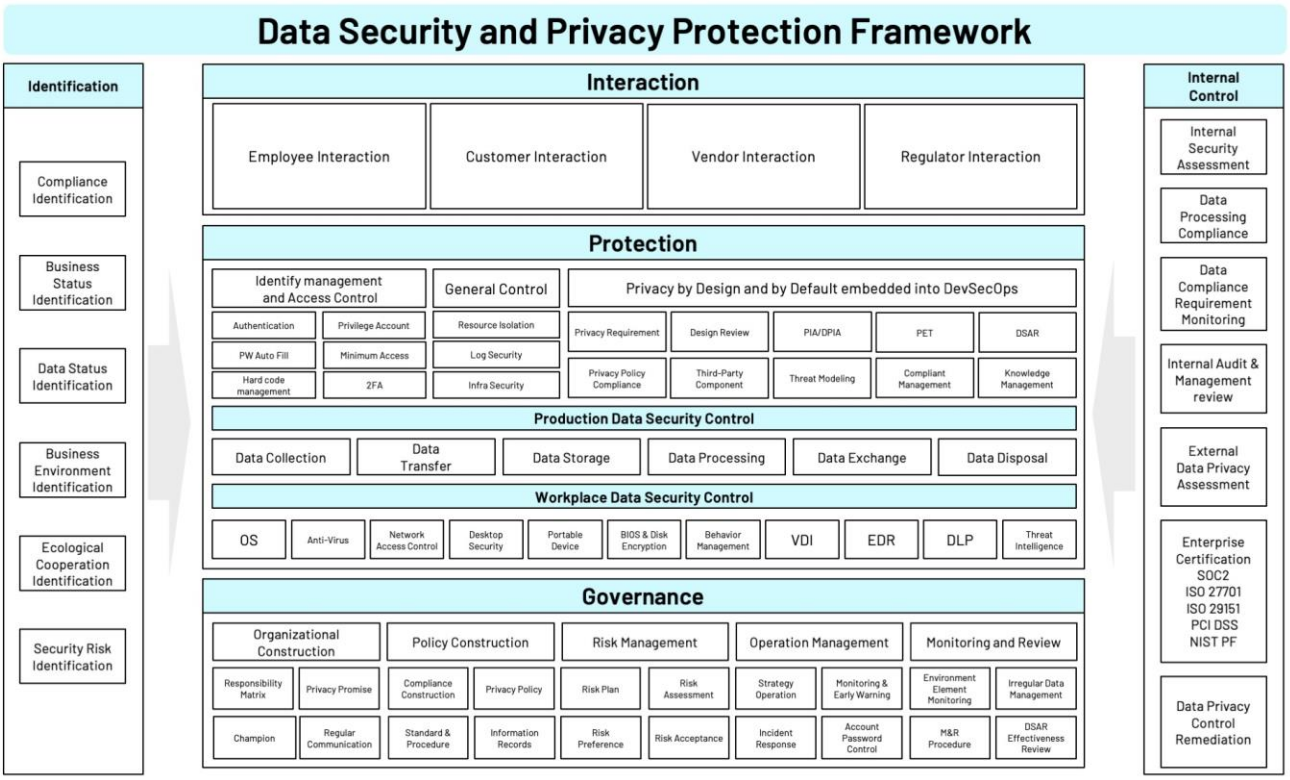

Figure: Data Security and Privacy Protection Framework

A framework for data security and privacy protection, organized into five modules, namely Identification, Governance, Protection, Interaction and Internal control.

A. **Identification module:** It is the beginning of the operation of the whole framework, through the continuous identification of laws and regulations, business status, data status, business environment, eco-cooperation and security risks, to fully understand the various types of bottom line accounts of the enterprise, which is the precondition for the operation of the data security and privacy protection framework;

B. Governance module: The governance module is the foundation of any system and consists of five key components:

    1) Organizational Construction: Improve the organizational structure, define data privacy responsibilities, and establish effective communication channels within the organization. Senior management should provide privacy commitments, and relevant systems and processes should be implemented through the data and privacy interface mechanism with business partners.
    2) Legal and Regulatory Compliance: Integrate data security and privacy protection laws and regulations into the governance framework. Establish a management system and process documentation to maintain records of implementation, ensuring compliance with applicable laws and regulations.
    3) Risk Management: Develop a comprehensive risk management plan for data security and privacy protection. Conduct risk assessments to identify potential risks and define the organization's risk tolerance and risk appetite, aligning them with the overall enterprise risk management framework.
    4) Data Security Operations and Management: Implement robust data security operations and management responsibilities. This includes effectively executing data security policies, monitoring and issuing warnings for potential threats, developing incident response procedures, and ensuring confidentiality controls are in place.
    5) Monitoring and Review: Establish a high-level monitoring and review mechanism to provide policy support for internal control measures. Conduct continuous monitoring of critical areas such as abnormal data reception, handling data subject rights, and monitoring environmental factors, ensuring ongoing compliance and identifying areas for improvement.

C. Protection Module: The protection module integrates identity management, access control, and general security controls from traditional network security and information security. In terms of data security, security control measures are built separately from the production environment and workplace office environment of the enterprise. The production environment builds control points based on the data security lifecycle of the DSMM, and the workplace office environment implements the corresponding security control measures according to the actual situation, establishes a cloud-native data leakage prevention system with isolation, blocking, and auditing, and effectively reduces the key, mnemonic, and other confidential data leakage risk of the Digital Asset Management Organization, credentials, codes, transaction strategies and other confidential data leakage risks of digital asset management organizations. In terms of privacy protection, the most important thing is to embed Privacy by Design (PBD) into the product development process of an organization;

D. **Interaction Module:** This module focuses on privacy protection and emphasizes the importance of communication between regulators, customers (data subjects), suppliers (data processors), and employees. Regulators need to maintain smooth two-way communication, provide appropriate approvals for cross-border transmission, fulfil notification obligations for data leakage, regularly disclose privacy reports, and enhance corporate responsibility. Customers should improve privacy notification, information, complaint and communication channels, manage customer consent, respond to data subject rights, and enhance customer experience. Suppliers need to implement due diligence, define responsibilities and obligations, conduct regular audits and reviews, maintain an effective incident response mechanism, manage SDKs and APIs, and maintain good communication. Employees should define their responsibilities, manage entry and exit, receive training, and follow reward and punishment management, communication management, and agreement management. Setting up a well-functioning Data Protection Officer (DPO) mechanism is critical to building a professional and effective communication contact point for data subjects and regulators;
E. **Internal Control Module:** Internal control is the Check and Action in the PDCA Deming Ring of management system, which is mainly to assess, check, verify and audit the operation effect of management system, obtain recognition from external organizations and professional qualification certification, and make continuous improvement through continuous preventive measures and rectification and corrective actions. The internal control module should be effectively integrated and connected with the network security or information security management system.

3.2.3.4.2 BUILDING A DATA GUARDIAN MATRIX WITH CLOUD-NATIVE AND SASE-BASED DATA LEAKAGE PREVENTION SOLUTIONS

To prevent the confidential and sensitive data leakage in the field of digital assets, digital asset management companies should establish a series of DLP protection measures that have mutual coverage and connection in the cloud, network, edge, and end. They should cooperate with AI-based security and intelligent management to enhance the ability of abnormal behaviour analysis, data visualization, and security insight. By using abnormal behaviour analysis, data visualization, and security insight capabilities, the DLP policy based on IPDRR (Identification, Protection, Detection, Responds and Recovery) provides continuous data discovery, leakage point update, policy update, and event disposal for daily data leakage prevention. The solution has the ability to detect and respond to internal mischief events in real-time, transforming it from a static stack of devices into an active approach that effectively prevents data leakage.

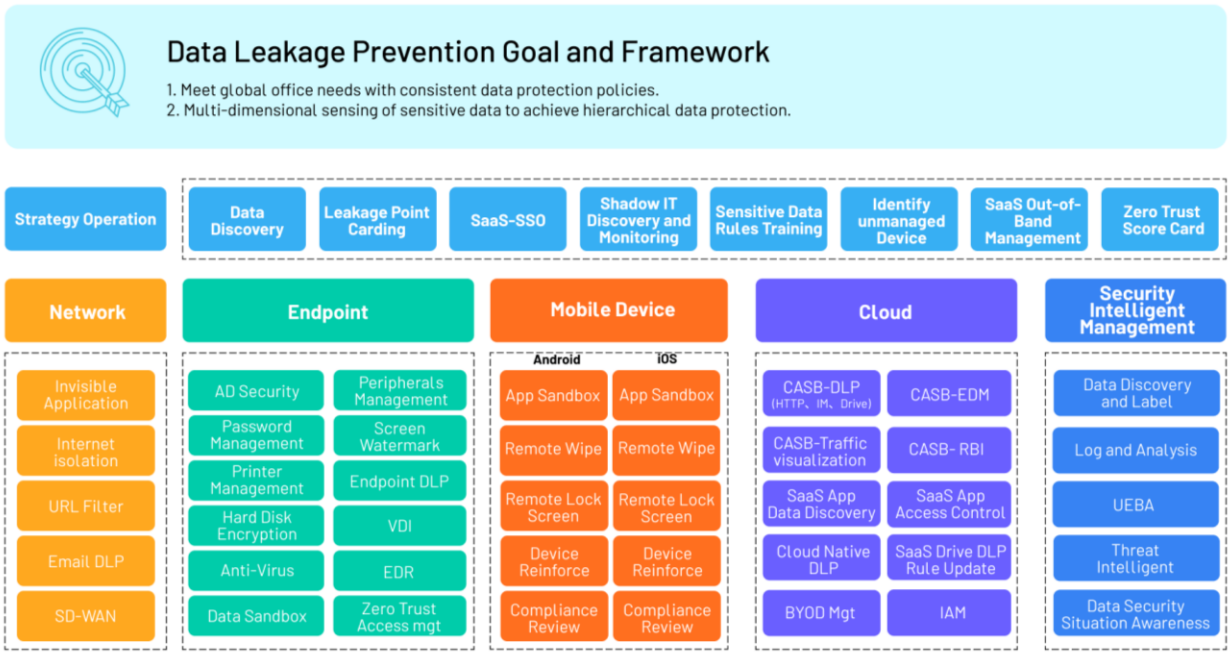

Figure: Data Leakage Prevention Goal and Framework

Cloud-native and SASE-based data leakage prevention solutions can comprehensively identify enterprise data leakage channels. They converge the data leakage surfaces of emails, chat software, file uploading websites, cloud disks, printing, self-installed software, BYOD, and Shadow IT, focusing on preventing and controlling only a limited number of data interaction channels. This solves the industry problem of converging data leakage points, which is key to achieving comprehensive data leakage prevention. To ensure effective operation, the data leakage prevention operation focuses on core contents at each link of IPDRR (Identification, Protection, Detection, Response and Recovery) for data leakage prevention:

- Identify
  - Data discovery, classification hierarchy and labelling;
  - Data usage scenario operations;
  - Data leakage risk assessment.
- Protect
  - Sensitive Data Rules Operations;
  - Terminal account privilege convergence & desktop control;
  - SaaS application exposure surface convergence;
  - SaaS application security settings;
  - API Continuous Integration for Cloud Native DLP;
  - URLs filtering rules operation;
  - Establishment of a data leakage prevention system to standardize and implement training and awareness-raising.

- Detect
    - Alarm monitoring;
    - Zero-trust endpoint detection;
    - AI-based UEBA detection;
    - SaaS breach detection.
- Respond
    - Employee Exit Check;
    - Data breach incident response;
    - DLP Policy Change Management;
    - Periodic reports.
- Recover
    - DLP Exception Release Management;
    - Troubleshooting.

Amber Group has continuously optimised its data leakage prevention efforts by implementing a comprehensive range of measures. These measures encompass organisational, technological, managerial, and operational aspects, effectively reducing the risk of unauthorised disclosure of sensitive information. This includes protection for passwords, credentials, access and secret keys, wallet keys, mnemonics, core code, customer data, and trade secrets associated with digital assets. By placing a high priority on safeguarding customer data and trade secrets, Amber Group maintains a strong and robust security framework.

3.2.4 BLOCKCHAIN GOVERNANCE SOLUTION

Whilst enabling technology to support Blockchain solutions is transformative, it is important to ensure that off-chain, appropriate governance protocols are in place. The ISO/TS 23635:2022 standard is used to establish the guiding principles and framework for the governance of distributed ledger technology (DLT) systems. This will enable data assets to be traded within appropriate risk management controls, which will help ensure appropriate safeguards are in place when technical issues occur. Blockchain governance also provides guidance on implementing governance, including risks and the regulatory environment, to support an effective, efficient, and acceptable use of DLT systems. Functionally, the following requirements are included:

- On-chain transactions record
- Stakeholder authorization for transactions
- Validation by the community according to predetermined rules
- Trusted trading chain platform

- Compliance requirements
- Extensible chain data
- Litigation management
- KYC (Know Your Customer)
- Authority management
- Transaction transparency
- Blockchain Security
- Rollback / Timeclock facilities

3.3 SECURITY CHALLENGE III: HACKING ATTACKS CONTINUE, STATIC COUNTERMEASURES LAG BEHIND AND GET BEATEN

3.3.1 INDUSTRY PAIN POINTS AND SECURITY THREATS

The blockchain is essentially a secure and trustworthy ledger in which the participants participate in bookkeeping together, and the potential uncontrollable risks associated with centralized bookkeeping are technically eliminated through consensus technology. Through the set consensus mechanism, the entire blockchain ledger abides by the set rules and operates continuously without being controlled by a certain or a small number of authoritative nodes, and the existence of this kind of technology makes cryptocurrencies using blockchain technology naturally come with a high degree of anonymity and difficult-to-trace characteristics.

However, because of this type of technology, once a user's private key or funds are stolen, it is very difficult to recover the corresponding funds. Hackers often exploit various technical means, including phishing, malware, and vulnerability exploitation, to target cryptocurrency users and service providers. This has led to notable security breaches, such as the incident in 2019 where a prominent cryptocurrency exchange experienced a significant attack resulting in the theft of approximately 7,000 bitcoins valued at around $40 million at that time. Despite the exchange's attempts to trace the flow of these funds, the stolen assets were ultimately unrecoverable due to Bitcoin's high level of anonymity and difficulty in tracing.

Pain Points and Threats 1: Key and mnemonic data leakage equals loss of funds on the chain

Theft or leakage of private keys and mnemonics is one of the main reasons for the loss of funds on the chain. This is mainly due to the high security risk and vulnerability of the cryptocurrency space. First, because blockchain is based on the principle of decentralization, the technical means to protect users' privacy is relatively weak, enabling information about users' behaviour on public networks to be widely recorded and tracked. This gives attackers the opportunity to access users' private information.

Furthermore, a significant security risk arises in the cryptocurrency space due to many users lacking awareness of the importance of properly managing their private keys and mnemonics. Often, these crucial pieces of information are stored on vulnerable devices such as computers, phones, or cloud services. In some cases, users may even write them down on paper or share them

with others, inadvertently exposing their cryptocurrency accounts to potential breaches. For users with large amounts of cryptocurrencies, any single information leak or security breach can lead to the loss of huge amounts of their property.

The reasons for the theft or leakage of private keys and mnemonics are varied and often involve both human and technical factors. Therefore, to solve this problem, it is necessary to approach it from multiple perspectives, strengthen the research and application of technical means, improve the security management mechanism of exchanges and users, and raise users' security awareness.

Pain Point and Threat #2: Hacker groups continue to attack and steal digital gold

Cryptocurrencies have received a lot of attention from various parties in recent years because of their huge rise in value, with BTC even being called digital gold, which shows the value of its objective existence. Because of this, the threat of continued attacks and theft by hacker organizations is a cause for concern. Although blockchain technology provides higher security, it is difficult to avoid hacker attacks. Currently, hacktivist groups use a variety of tactics, including social engineering attacks, phishing, and malware, to try to gain access to users' wallets or exchanges and steal their private keys or mnemonics in order to obtain digital gold. In recent years, many major incidents have shown that hacker groups have broken into the systems of some of the major cryptocurrency exchanges and managed to steal millions of dollars of digital gold.

Pain Points and Threats 3: Potential Insider Trust Risks Based on Cryptocurrency Characteristics

Cryptocurrencies, with their characteristics of decentralization, anonymity and non-tamperability, make them a safer digital asset. However, also because of its characteristics, there is a potential threat of insider trust risk. In particular, security issues arise when employees of cryptocurrency companies or exchanges abuse their privileges and leak user information and private keys to others, and because of the nature of cryptocurrencies, it is relatively difficult to prove and investigate to some extent.

For example, in 2019, cryptocurrency exchange Binance suffered a hack and was allegedly caused by a leak from one of its employees. The incident brought to light the fact that even with the protection of blockchain technology, digital gold is still subject to internal trust risks.

Pain Points and Threats 4: Embracing Various Security Compliance Requirements Under Regulation

Security compliance has emerged as a pressing concern for the cryptocurrency industry as governments and regulators worldwide tighten their oversight of the digital gold market. Regulators in many regions require cryptocurrency companies and exchanges to comply with a variety of security compliance requirements, such as KYC (Know Your Customer) regulations, AML (Anti-Money Laundering) regulations, CFT (Combating Financing of Terrorism) laws, and more. These related compliance monitoring requirements likewise pose a higher challenge to the security management of digital assets.

3.3.2 REGULATORY REQUIREMENTS FOR DIGITAL ASSETS IN THE AREA OF CYBERSECURITY

Countries and jurisdictions such as Hong Kong, China, Singapore, Japan and South Korea have respectively put forward cybersecurity-related requirements in their digital asset compliance licenses, including the Virtual Asset Service Provider (VASP) in Hong Kong, the Monetary Authority (MAS) in Singapore, the Financial Services Agency (FSA) in Japan and the Korea Internet Security Agency (KISA). Digital asset management companies should identify the digital asset compliance requirements of these jurisdictions while building security attack and defense countermeasure solutions, and implement corresponding cybersecurity compliance controls as required.

3.3.2.1 CYBER SECURITY REQUIREMENTS FOR VIRTUAL ASSET SERVICE PROVIDERS (VASPS) IN HONG KONG, CHINA

Hong Kong's Virtual Asset Service Providers (VASPs) have explicitly emphasized the need for comprehensive security measures in various areas, including customer virtual asset custody, basic security requirements, platform security, platform adequacy, platform reliability, platform capacity, and contingency measures. The cybersecurity requirements of Hong Kong's Virtual Asset Service Providers (VASPs) basically cover many aspects of traditional cybersecurity and information security governance, and also incorporate the characteristics of the digital asset business, with additional extended requirements for digital asset hosting, wallet security, and blockchain security, which poses a huge challenge for companies unfamiliar with traditional cybersecurity as well as those that do not understand the security characteristics of digital assets.

The key elements of cybersecurity for Hong Kong's Virtual Asset Service Providers (VASPs) are listed below:

- Custody of Client Virtual Assets: The requirements for custody of client virtual assets in Hong Kong entail that platform operators and associated entities should, in most cases, store 98% of client virtual assets offline. This offline storage is typically implemented using Hardware Security Modules (HSMs) to minimize the risk of losses resulting from platform intrusions or hacking incidents. Additionally, the requirements outline stringent security measures in various control domains, such as cryptographic seed randomness, key lifecycle management, localized storage of seeds and private keys, wallet security control, and on-chain threat intelligence.
- Basic Security Requirements: The focus of this security domain is to require enterprises to establish a cybersecurity governance system to ensure reasonable planning, implementation, operation, monitoring and continuous improvement of the cybersecurity governance system. It includes general principles, resource security, personnel requirements, role responsibilities, outsourcing management, supply chain management, cross-departmental cooperation, internal reporting, governance mechanisms, monitoring and correction, independent auditing and other related requirements;

- Platform Security: The security requirements of this security domain reflect a combination of traditional network security and digital asset features, including identification, authentication, access control, data and document access, permission change, permission review, access date and application record, data change, data leakage prevention, data misuse prevention, data monitoring, two-factor authentication, password management, login failure detection, session timeout monitoring, account abnormal notification, customer security notification, security monitoring, network isolation, remote access, vulnerability and patch management, anti-virus management, intrusion prevention and detection, endpoint detection and response (EDR), security information event management (SIEM), security operation center (SOC), software and hardware whitelisting management, physical environment security management, data storage and transmission encryption, application system monitoring, security training. A number of complex security technology system requirements, such as publicity, risk assessment, incident response and notification;
- Platform Adequacy: Virtual asset platform operators are required to ensure the robustness of their platforms by maintaining a high level of reliability, security and capacity of their systems, with appropriate contingency measures in place.
- Platform Reliability: Virtual asset platform operators are required to have written standard operating procedures for system upgrades and maintenance.
- Platform Capacity: Requirements in the platform capacity management, including capacity monitoring, recording, stress testing, system and data backup and recovery, contingency plans and other requirements.
- Contingency Measures: Organizations are required to establish robust management mechanisms and practical capabilities in business continuity to ensure that the business can continue to operate effectively, with specific requirements including the formulation of plans such as BCPs and DRPs, the establishment of contingency plans, and the requirement to conduct regular contingency drills.

3.3.2.2 CYBER SECURITY REQUIREMENTS OF THE MONETARY AUTHORITY OF SINGAPORE (MAS)

The Monetary Authority of Singapore (MAS) currently (as of June 2023) regulates the digital currency trading market under the powers granted by the Payment Services Act, and licensees are required to comply with the authority's Technology Risk Management or TRM guidelines. Among the cybersecurity related highlights are as follows:

1) Security Measures: Financial institutions must implement appropriate security measures to protect their network systems and communication facilities from unauthorized access, malware and other cyber-attacks. This includes requirements such as firewalls, intrusion detection and defense systems, and anti-virus software;
2) Network Access Control: Financial institutions should implement strict network access control mechanisms to ensure that only authorized users have access to sensitive data and systems. This may include authentication, access rights management, multi-factor authentication, etc.;
3) Network Monitoring and Incident Response: Financial institutions need to implement network monitoring and incident response mechanisms to detect and respond to cyber security incidents in a timely manner. This includes real-time monitoring of cyber activity, logging, threat intelligence analysis, etc., as well as the establishment of an effective incident response plan;
4) Data Protection and Encryption: Financial institutions must take appropriate measures to protect the confidentiality and integrity of sensitive data stored and transmitted. This may include data encryption, key management, secure transmission protocols, etc.;
5) Employee Security Awareness: Financial institutions should raise employee awareness of cybersecurity and help them identify and respond to potential cybersecurity threats, including social engineering attacks, phishing emails, etc., through training and educational activities;
6) Third-party Vendor Security: When working with third-party vendors, financial institutions must ensure that their cybersecurity controls are compliant and monitor the vendor's security measures. This may include conducting security audits and due diligence on the vendor to ensure that it is able to provide standards-compliant cybersecurity protection;
7) Compliance and Reporting: Financial institutions are required to comply with MAS's cybersecurity regulatory requirements and report any significant cybersecurity incidents or breaches to MAS in a timely manner.

3.3.2.3 CYBERSECURITY REQUIREMENTS OF THE FINANCIAL SERVICES AGENCY (FSA) OF JAPAN

Japan, as one of the countries that actively embraced digital assets earlier, began to formally introduce a registration system for digital asset trading platforms on April 1, 2017, through the Amendment to the Funds Settlement Law. Japan's digital asset regulatory bodies mainly contain three categories, namely the Japan Financial Services Agency (FSA), the administrative regulator; the Japan national tax agency, which formulates the digital asset tax system and implementation rules; and the Japan Virtual and Crypto assets Exchange Association (JVCEA), which actively promotes industry autonomy and self-regulation. This means that digital asset activities in Japan need to meet the compliance requirements of all three regulators in terms of asset transactions, business activities and security operations.

In particular, the Japan Financial Services Agency (FSA) and its Japan Virtual and Crypto assets Exchange Association (JVCEA) have put forward the following requirements on cybersecurity management for digital asset management companies registered in Japan:

1) Security risk management of platforms and systems: This area focuses on the requirement for registered entities to control the security risks of business platforms and systems as a whole, with emphasis on, for example, the development of security risk assessments and the formulation of risk response policies and strategies, the identification of security risk management organizational structures and personnel, and the formation of an effective PDCA (Plan-Do-Check-Act) management posture, and so on;
2) Data security management: This area focuses on the requirement for registered entities to take reasonable and effective detection and prevention measures to protect the confidentiality, integrity and availability of data. These initiatives include the development of encryption procedures, safekeeping of secret keys, secure data access controls, etc.;
3) Network threat management: This area requires registered entities to formulate a multi-level network security defense system based on risk analysis, and to make timely adjustments to personnel organization and preventive technology means in the light of internal and external network threats. Personnel organization system construction includes effective detection, reporting and response communication systems. Preventive technology means include intrusion detection and intrusion prevention, real-time threat monitoring, network isolation, and regular implementation of third-party vulnerability testing;
4) Security Assessment and Reporting: This area requires registered entities to conduct self-tests and assessments of cybersecurity and to receive regular inquiries and inspections from the Japan Financial Services Agency (FSA), which include submitting self-test and assessment information on a regular basis and receiving on-site inspections of the physical environment from the FSA. At the same time, the JVCEA sends a self-evaluation questionnaire to registered members on a regular basis, and registered entities are required to fill out the questionnaire in accordance with the actual situation and take action in response to the risk alerts. Any cybersecurity incidents should be reported to the FSA in a timely manner;

5) **Asset Custody Security:** In order to safeguard the security of digital asset custodianship, the Japan Virtual and Crypto assets Exchange Association (JVCEA) has imposed strict self-governance requirements, such as: the target value of the ratio of hot and cold wallet storage should be set for the management of customers' assets, and the numerical target thresholds should be reviewed periodically; Preventive and monitoring measures should be taken to prevent abnormal internal and external use of hot and cold wallets and their management systems; technical means should be adopted to prevent unauthorized intrusion; access to wallet private keys should be controlled, such as implementing IP address restrictions, terminal physical access restrictions, and multifactor authentication; and strict autonomy requirements have been put forward with respect to random number generation of the seed key and on-chain attacks;

6) **Incident Response and Business Continuity:** Influenced by the geographical factors in Japan, in terms of cybersecurity requirements, Japan's Financial Services Agency (FSA) focuses on the need for registered entities to have better incident response and business continuity management. Detailed items such as the establishment of a management organization with DRP and BCP, communication mechanism, incident response process and business continuity system management policy; at the same time, it should regularly implement incident response drills for high-risk scenarios such as cyber-attacks, recovery of digital asset custodian wallets, loss of digital assets, and so on.

3.3.2.4 CYBERSECURITY REQUIREMENTS OF THE KOREA INTERNET SECURITY AGENCY (KISA)

The South Korean government has gradually escalated its regulation of virtual assets in recent years and issued the Specific Financial Transactions Information Reporting and Use Act (SFTR, Special Financial Transactions Information Act) in January 2018, which requires virtual currency exchanges to implement a real-name system and to submit relevant transaction information. In March 2020, the National Assembly of South Korea passed the Specific Financial Transactions Reporting and Use Act (SFIA, Special Financial Transactions Information Act), which regulates virtual asset service providers (VASPs) and imposes anti-money laundering (AML) obligations on them. In addition, the Act provides a definition of virtual assets to better regulate them. 2021 On March 25, 2021, the Korean government amended the SFIA Act to further strengthen the regulation of VASPs and to require VASPs to report transaction information to financial regulators, and to require that all Virtual Asset Service Providers (VASPs) be certified by the Korean Information Security Management System (K-ISMS). certification.

K-ISMS is a standard for assessing whether businesses and organizations are operating and managing their information security management systems consistently and securely to thoroughly protect their information assets. The standard's requirements for cyber security focus on the following areas:

1) Establishment and application of management system: Institutions should establish a comprehensive information security management system, covering levels including the establishment of organizational structure, system construction, information security risk management process, independent audit function, and continuous supervision and self-inspection and rectification process.
2) Policy, organization and asset management: The agency clearly defines and delineates roles and responsibilities related to information protection and personal information protection. In addition, depending on the use and importance of information assets, handling procedures and protection measures must be established and implemented, and the responsibility and management of each asset must be clarified. Segregation of duties standards must be established and implemented to prevent potential damage caused by misuse or abuse of authority.
3) Cryptocurrency wallet system security management: Institutions should establish a comprehensive wallet security management process, and conduct a full review of the wallet system architecture to ensure the security of the private key in the process of generating, slicing, storing, backing up, and recovering. During the design phase of the wallet system, detailed security requirements (construction of multi-signature mechanism, network control and whitelist setting, unspecified IP/PORT communication, transaction result verification, etc.) should be formulated, and careful testing and pre-launch verification should be conducted. In addition, the institution shall properly store the wallet infrastructure equipment and deploy appropriate physical security controls to ensure that the wallet equipment is monitored, accessible to specific personnel, and protected by multiple physical layers to prevent it from malicious damage, theft, and unauthorized access.
4) Data encryption: To protect personal and critical information, organizations should establish encryption objectives, password strengths, and password usage policies reflecting legal requirements. Encryption should be applied when storing, transmitting, and communicating personal and critical information. At the system application level, organizations should establish and implement procedures for managing the secure generation, use, storage, distribution, and destruction of encryption keys. They should also develop a recovery plan when necessary to ensure secure management of encryption at all times.
5) Information system introduction and development security: When introducing, developing and changing information systems, organizations should define and apply security requirements, such as legal requirements related to information protection and personal information protection, the latest security vulnerabilities and secure coding methods. Before going live, it shall undergo comprehensive security testing, including but not limited to vulnerability scanning, source code auditing, and penetration testing, and shall take improvement measures and perform retesting to confirm any security issues found.
6) Security Operations and Response: The organization should establish and implement detailed security operations procedures, such as assigning administrators by security system type, updating policies, changing rule sets, monitoring events, and managing the current status of security system policy applications. They should also establish systems and procedures for detecting, responding to, analysing, and sharing internal and external infringement attempts.

This includes developing a cooperative system with relevant external organizations and experts to prevent intrusion incidents and personal information leakage, and responding quickly and effectively in the event of an incident. To quickly detect and respond to internal/external infringement attempts, personal information leakage attempts, cheating, etc., the organization must collect and analyse network and data flow and take timely follow-up measures based on monitoring and inspection results.

3.3.3 STORY 1: CRYPTOCURRENCY EXCHANGE COINCHECK ATTACKED AND STOLEN

In 2018, Coincheck disclosed that its escrowed assets had been stolen by hackers, and according to a post-event investigation this incident was caused by Coincheck's private keys being stored on an internet-connected computer without the use of a more secure cold wallet storage method. Hackers exploited a vulnerability in Coincheck's system and managed to steal NEM digital currency from user accounts and transfer it to another address.

Coincheck is one of the largest cryptocurrency exchanges in Japan, it was founded in 2014 and obtained a license from the Japanese Financial Services Authority in 2017. However, Coincheck did not take adequate security measures to protect its systems and users' assets, which led to this major digital currency theft.

This incident has brought Coincheck huge losses and a credibility crisis. Japan's Financial Services Agency investigated Coincheck and took administrative measures to penalize it, and Coincheck has also indicated that it will provide compensation to affected users and gradually restore its business.

The incident brought attention to the security challenges that digital currency exchanges face and the need for stronger regulation and supervision in the cryptocurrency industry. Since then, many countries have embarked on stricter regulatory measures for digital currency exchanges and the cryptocurrency industry.

3.3.4 STORY 2: THE CONTINUING CONFRONTATION OF STATE-LEVEL APT HACKING ORGANIZATIONS

The number of security events that the security team of a digital asset management company needs to detect and respond to in a timely manner will continue to increase, including, in particular, attacks from world-renowned hacking organizations, national-level hacking teams, and other attack activities.

Taking Amber Group as an example, the overall security architecture and operation system of Amber Group has been optimized in the direction of being more adaptable in the process of uninterrupted and continuous exchange.

In a month of 2020, Amber Group's security department received an alert from the UEBA module, and the security operation team immediately intervened to investigate and respond, and found that an employee account had carried out an abnormally sensitive behavioural operation under circumstances other than his own. Security incident response personnel immediately launched an in-depth analysis and investigation of the relevant terminal and network pairs, and determined that a national APT organization on our company's targeted attacks. The principle of the attack is as follows: Firstly, the attackers targeted specific employees of the company and conducted precise social media or external network phishing campaigns. They employed sophisticated methods to establish a backdoor link without raising suspicion. Subsequently, they proceeded to steal encrypted credentials from the compromised employees' terminals. By decrypting these legitimate credentials, the attackers gained unauthorized access and conducted internal actions in an attempt to obtain valuable information. The security team relied on accurate behavioural analysis technology to quickly locate the anomalies and respond to the breakthroughs and failures of the first half of the defence line (targeted phishing breakthroughs, no-kill construction of backdoor links) and cut off the backdoor links in a timely manner, successfully blocking the corresponding attack attempts.

From past experience, purely exogenous additional defense capabilities and how "brick wall" in theory, there is also the possibility of iterative breakthroughs by more advanced technology, combined with the endogenous immune-type anomalous behaviour analysis capabilities combined with exogenous "brick wall" is one of the best means to continuously The combination of endogenous immune-type abnormal behaviour analysis capability and exogenous "brick wall" is one of the best means to ensure the effectiveness of security.

3.3.5 INDUSTRY SECURITY SOLUTIONS PRACTICES

When facing external security threats, digital asset management companies should build a traditional network security and Web3 security operation system with the elements of **"Prioritize Compliance"**, **"Focus on Defence"** and; **"Attack to Defend".** Simultaneously, internally, they should aggregate and analyse various behavioural trajectories and operation records of users and employees to proactively identify potential risks and detect instances of identity theft or impersonation. By implementing detailed automated behavioural analysis, the security team can promptly discover potential internal operational risks and identity theft attempts, ensuring a swift response.

3.3.5.1 VERTICALLY INTEGRATED NETWORK SECURITY SYSTEM

The security construction of the digital asset management company mainly focuses on three major aspects of construction: Security Defence Infrastructure Deployment, Knowledge- and Intelligence-based Security Operation, and Actual Combat-based red and blue confrontation.

3.3.5.1.1 SECURITY DEFENCE INFRASTRUCTURE DEPLOYMENT

"Prioritize Compliance", is the guiding principle of cybersecurity defense infrastructure deployment, to ensure that the cybersecurity defense infrastructure achieves a higher level of construction on top of the compliance requirements of each jurisdiction, and detects and protects the multi-dimensional deep space from inside and outside the network boundary to the endpoint level.

- **Network border:** to build and deploy firewall as the core, and on it to build controllable security channel VPN, VDI and synchronized in the Internet space to introduce cloud WAF for remote data cleaning and content distribution;
- **Network Link Layer:** DPI devices are deployed for in-depth inspection of network layer IPS and bypass traffic to enable inspection and intelligence detection at the network link layer;
- **Business Organization Layer:** PAM-based control of unique legal operation and maintenance channels and simultaneous deployment of organizational defence software (ADI, HoneyNet);
- **Business Operation Layer:** Aggregate and collect relevant audit logs according to demand to support subsequent platform-based behavioural analysis;
- **Terminal Management Layer:** Deploy multiple security applications of different nature at the terminal level, including EDR, MDE, EPP, CASB, DLP, etc., to monitor and protect the working environment of users and applications in multiple dimensions.

3.3.5.1.2 KNOWLEDGE- AND INTELLIGENCE-BASED SECURITY OPERATIONS

Knowledge- and intelligence-based security operations have become a necessary means of maintaining information security. This type of security operation model, which focuses on collecting, analysing and applying all kinds of information and knowledge, can help enterprises to better identify and manage risks, respond to security events, optimize security controls, etc., and to target and efficiently defend against key objects by means of ahead-of-the-curve threat intelligence information, reflecting the idea of network "Focus on Defense".

The realization of knowledge- and intelligence-based security operations requires the establishment of sound information collection and processing mechanisms. Cybersecurity technologies, sensors and other monitoring devices are used to obtain information relevant to their business, such as types of attackers, attack methods, vulnerabilities, user behaviours and so on. At the same time, organizations also need to leverage various sources of information, such as government, partners, vendors, social media, etc., to obtain more comprehensive information.

Amber Group has accumulated vast knowledge and intelligence from various sources, coupled with extensive industry experience. This has enabled us to develop numerous advanced analysis and detection rules and strategies that are specifically tailored to the digital asset industry. Through remote real-time synchronization with various types of machine-readable intelligence, Amber Group can provide real-time hit-matching capabilities that help detect potential threats quickly. This enables our clients to proactively defend against cyber-attacks and maintain a stronger security posture.

3.3.5.1.3 ACTUALIZED AND REGULARIZED RED AND BLUE CONFRONTATIONS

"Attack to Defend" is a core tactic of traditional and Web3 cybersecurity that focuses on conducting regular live red-blue confrontations. Live red-blue confrontation is a training and assessment methodology that simulates cybersecurity threats to evaluate an organization's defences. It involves adversarial simulations that help organizations identify and address possible vulnerabilities, test incident response plans, and enhance security team capabilities.

A red-blue confrontation typically consists of red and blue sides. The red side represents potential external or internal attackers attempting to penetrate systems and steal sensitive data or cause damage. The blue side represents defenders who must detect intrusions, fix vulnerabilities, and respond to incidents.

Conducting regular red-blue simulations has significant value for enterprise information security. It allows organizations to find system vulnerabilities in a controlled test environment without affecting production systems. Red-blue confrontation also helps evaluate security policy effectiveness by identifying existing gaps and drive improvements. Importantly, these simulations strengthen collaboration and communication among security teams, improving readiness for cyberattacks.

Amber Group has built a deeply integrated network infrastructure and security operation mechanism based on knowledge intelligence and have partnered with internal and external red teams to conduct periodic red and blue confrontation drills. For example, we have invited the SlowMist red team to participate in these drills, which are designed to identify deficiencies and weaknesses in the operation mechanism of our depth of protection. Through these combat-oriented drills, we can refine the capabilities of our teams and platforms and promote defense by attacking.

3.3.5.2 LABYRINTH-BASED ACTIVE DEFENSE MECHANISMS

Deception maze based active defense mechanism is an active defense method against network attacks, in which honeypot technology is one of the core means. Honeypot is a special virtual environment that simulates all kinds of services and applications in the real system, but does not contain any real business data and user information, so it can be used to attract attackers to enter and collect attack intelligence from them, in order to set up a "private intelligence sharing network for hackers touching the network", and share hacker details instantly once the hackers have entered the network or obtained sensitive decoy files. Once a hacker has entered the network, or obtained sensitive decoy files, hacker details can be shared instantly, providing the digital asset industry with proprietary and valuable threat intelligence to take necessary action in a timely manner.

The main value and significance of active defense based on honeypot technology is:

1) Provide Early Threat Detection: By setting up honeypots, enterprises can detect potential threatening behaviours, such as system scanning, port scanning, and vulnerability exploitation, earlier and take timely action;
2) Deceive Attackers: Honeypots can deceive attackers into thinking that they have successfully entered the target system, thereby reducing their attack efficiency and destructive capability;
3) Collecting Attack Intelligence: By collecting the activities of attackers through honeypots, enterprises can obtain rich security intelligence, such as attackers' attack methods, attack tools, and attack sources, in order to analyse and improve overall security;
4) Analysing Attack Behaviour: Honeypot technology can help companies identify attackers' methods and patterns of attack, so they can better understand security threats and take more effective defensive measures.

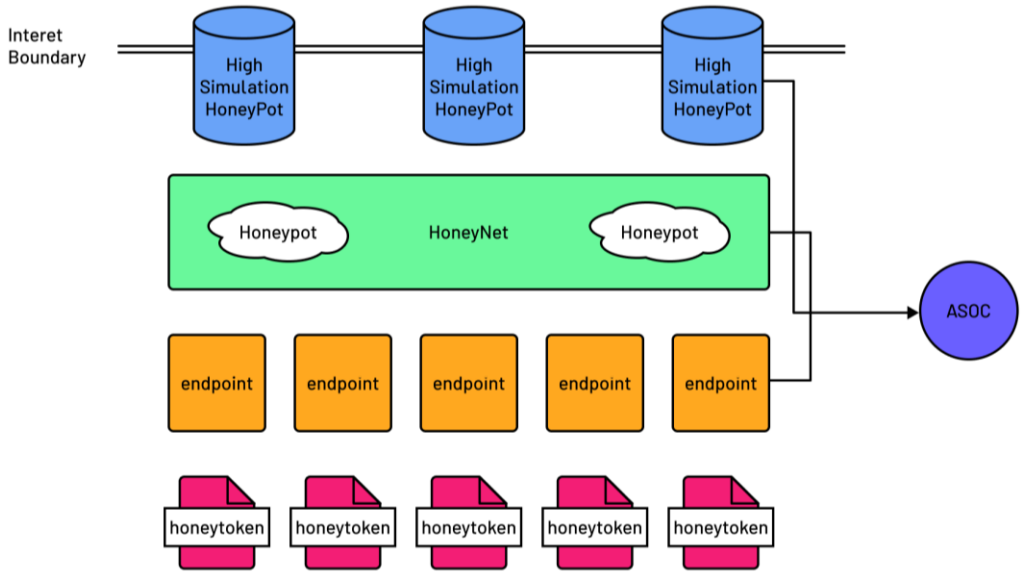

Figure: Labyrinth-based active defense mechanisms

Amber Group utilizes multiple forms of trapping and detection mechanisms, including Platform Honeynet, High Simulation Honeypot, and Honeytoken. These mechanisms are integrated with our intelligence operation platform to provide full monitoring and automated response to potential attackers, ensuring robust protection of the platform's digital assets.

3.3.5.3 MALICIOUS BEHAVIOR ANALYSIS BASED ON UEBA TECHNOLOGY

Malicious behaviour analysis based on UEBA technology is an advanced threat detection and response method for network attacks, and its core idea is to analyse information such as user behaviour and network traffic through intelligent algorithms and machine learning techniques to discover potential security threats and take timely measures to deal with them.

UEBA technology is able to achieve the following capabilities when analysing massive logs based on access:

1) **Detecting Unknown Threats:** Compared to traditional rule- or signature-based threat detection methods, UEBA technology is more flexible and intelligent. It can identify abnormal behaviours that do not fit normal user behaviour patterns, thus discovering unknown attacks and insider threats;
2) **Optimizing Security Decisions:** UEBA technology can help organizations better understand their security risk profile. The results of the analysis can be used to extrapolate risks, develop security policies, optimize security controls, and more, enabling organizations to make better security decisions;
3) **Improved Security Efficiency:** UEBA technology utilizes machine learning algorithms that are faster and more efficient than traditional methods. It can adaptively learn new attack models and vulnerabilities and automatically adjust defense strategies, thus dramatically improving security efficiency;
4) **Enhanced Security Situational Awareness:** UEBA technology can integrate and analyse data from different sources to form a global security situational awareness. By monitoring and analysing the behaviour of the entire network, enterprises can detect and respond to unknown attacks in a timely manner and gain useful intelligence from them.

Based on security requirements, Digital Asset Management aggregates various types of logs, including user behaviour audit logs, VPN login access audits, critical application operation audits, etc., and efficiently achieves the ability to sense and hit unknown threats and potential lurking attackers by learning and modelling historical data and detecting them in real time at the present time.

The specific operation process is as follows:

Access to audit logs containing user action activities, the algorithm analyses and extracts content from the logs, including time, user, operation, status and other core fields, and constructs an operational model for describing user objects from the input training data by means of algorithms such as statistical learning, clustering analysis, and deep neural networks; the algorithm is about to use this user model for pattern matching on the corresponding users occurring in real time in order to detect relevant potential risky anomalous operations.

3.3.5.4 AUTOMATED INTELLIGENT RESPONSE FOR SOAR & AI

Incident response has been a vital component of security management in both traditional and emerging industries which include digital assets. The primary objective of incident response is to mitigate damage. When a security incident occurs, an effective incident response mechanism ensures that the organization is ready to take prompt actions to contain the security incident such as isolating affected systems. This not only aids in minimizing the loss of information assets but also reduces the duration of business disruption.

Furthermore, an efficient incident response can offer valuable post-incident analysis. This analysis typically uncovers the attacker's techniques and tactics, as well as the organization's defensive weaknesses. Armed with this information, organizations can address vulnerabilities and refine their security policies to prevent similar incidents from recurring in the future. Additionally, incident response plays a crucial role in meeting regulatory compliance requirements. Numerous industry-specific and regional regulations mandate organizations to report and take appropriate measures in the event of a security incident. By implementing an effective incident response mechanism, organizations can fulfil these compliance and regulatory requirements.

In summary, an efficient and effective incident response mechanism not only reduces the potential damage to the organization resulting from a security incident but also enhances the organization's overall security posture to meet regulatory and compliance requirements.

Amber Group has established comprehensive incident response mechanisms. A core element is their SOAR & AI automated intelligent response platform, that detects issues autonomously and swiftly takes appropriate remedial action through automated workflows and intelligence. This enables more efficient incident response with less burden on security teams.

SOAR, or Security Orchestration and Automation, is a solution specifically designed to assist incident response teams in seamlessly integrating internal and external systems, thus enabling them to address security incidents effectively and promptly. The process entails gathering extensive data on security alerts and incidents, consolidating and analysing the information, and automating the implementation of security procedures to manage these incidents. This automation significantly enhances the security teams' efficiency, reduces labour expenses, and minimizes the risk of human error.

Simultaneously, by utilizing a vast array of historical event alerts, threat intelligence, and past processing outcomes as a dataset for fine-tuning an AI-based model, the system can swiftly filter out false positives and accurately pinpoint genuine threats. This capability effectively improves an organization's overall security defences. Digital asset management companies can combine SOAR and AI technologies to achieve the following goals:

1) Automation and Orchestration: SOAR is able to process and analyse security alerts and event data from various data sources and action on them using pre-built playbooks. The playbooks are created from the security team's expertise on incident handling and are typically integrated with various internal and external systems, including log repositories, intelligence platforms, endpoint management, vulnerability management, network management, identity and privilege management, cloud platforms and instant messaging for data enrichment, incident triage and remediations.
2) Accurate Triage and Timely Response: AI has proven its ability to support the incident handling process. Utilizing historical security alerts, remediation steps, and threat intelligence as inputs, fine-tuned AI models are able to assist the security team in swiftly triaging security alerts and automatically identifying high-risk alerts. Combining the benefits of SOAR and AI, the system can quickly identify security threats and automate responses, significantly reducing the time from threat detection to resolution and effectively mitigating security risks.
3) Continuous Learning and Improvement: Capitalizing on SOAR's integrated log analytics platform and AI, continuous learning is conducted based on previous security event data. This process assists the security team with post-incident analysis and summarization, refining the results into action lists that are then fed back to the various engineering teams for follow-up, forming a closed-loop system.

3.3.5.5 DIGITAL FORENSIC SOLUTION

As cases of fraud, bribery, and illicit transactions related to digital assets are on the rise, litigation and arbitration involving digital assets and blockchain technology have also become a rapidly growing part of the legal landscape. Although security management of digital assets is getting more and more advanced, it cannot perfectly meet the needs of all circumstances. In many litigation cases, enterprises and related partners must ensure that the investigations and practices conducted strictly follow the electronic evidence discovery workflow and standards recognized by laws and regulations. Therefore, in addition to the assistance of the legal counsel, it is also crucial to retain forensic experts to collect and analyse electronic evidence from a forensic perspective. Throughout the life cycle of electronic evidence discovery, forensics experts will strictly preserve the evidence following a complete chain of custody practices, record every step in the process, and use legally recognized tools for the analysis. If important information is omitted during the investigation, the analysis findings may lose the expected evidentiary effect in front of the regulation or the court trial.

Ankura provides forensic preservation and analysis of electronically stored information (ESI) to various industries, including the cryptocurrency field, to support litigation, arbitration, investigation, internal review, etc., or to provide expert testimony in court proceedings. Ankura experts have experience in participating in litigation related to digital assets in the United Kingdom, the United States, Singapore, and Hong Kong, and provide expert witness reports and testimony for complex digital asset litigation and regulatory investigation. Ankura can also provide advice and services in other judicial systems that accept expert witnesses.

3.3.5.6 CRYPTOCURRENCY RISK CONTROL THROUGH INSURANCE

Whilst offering cyber insurance within the digital assets space is still emerging and deemed high risk for many insurers, several long-term players have entered the market willing to provide limited coverage against typical cyber and IT exposures.

Given the risks associated with crypto currency assets, necessary measures should be actively taken to protect these assets. Insurance is an emerging option for covering security risks, but it can be challenging to obtain without demonstrating the maturity of a company's security and IT controls environment to insurers' standards. Some cryptocurrency exchanges and cryptocurrency custodians may provide insurance for their services, but in addition to what these entities provide, supplemental insurance may be required to adequately control crypto currency-related risk exposures. The relevant insurance can be written into a stand-alone policy or included in general commercial insurance, such as cyber insurance, IT insurance and/or commercial crime insurance. Cyber security insurance provides protection against security or privacy breaches such as cyberextortion, data extraction, cyber-crime and ransomware attacks. It may provide some coverage for data breaches that hackers steal or try to steal crypto currency from online wallets. For example, an insurance policy may cover expenses associated with hiring a computer forensics professional to determine the cause of the loss and terminate the attack or for legal representation when responding to regulatory enquiry or third-party disputes. A cyber security

insurance policy can also help you recover your data and cover lost revenue due to business disruption as a result of cyber-attacks and data breaches. However, cyber security insurance typically does not cover "money" or "securities" losses. Commercial crime insurance is another avenue to follow which provides loss protection related to crimes such as theft and fraud.

Ankura partner with many Cyber Insurance companies as part of their global forensics and incident response panels, working with crypto software and hardware providers seeking technology due diligence exercises to enable them to gain cyber insurance from their insurance carrier for their solutions. Technology solution overviews are often undertaken, assessing the security architecture of the solution and documenting best practice implementation guides to reduce the attack surface when deployed on customer sites.

3.4 SECURITY CHALLENGE IV: FROM CHAOTIC AND BARBARIC GROWTH TO COMPLIANT AND REGULATED SUNNY DEVELOPMENT

3.4.1 INDUSTRY PAIN POINTS AND SECURITY THREATS

After more than a decade of development, the digital asset industry has gradually come out of the haze from the unregulated chaos, and global regulators have also been actively building compliance frameworks in recent years to address the profound impact and great challenges of digital currencies on the global financial system, to reduce money laundering, terrorist financing and security risks, to establish a more open and transparent regulatory environment, and to protect the rights and interests of investors, enterprises and other participants, and to help the industry's sunshine development.

Major economies around the world are aware of the importance of regulating digital assets and have begun to try to legislate and build compliance frameworks. For example, Singapore, Japan and Hong Kong, China, which are crypto-friendly jurisdictions in Asia, have a clearer attitude towards regulation and have specific regulatory frameworks, licensing regimes or permit systems for digital assets. Individual states in the U.S. have different attitudes towards digital assets, with Washington and New York having clearer regulations and licenses, while the U.S. Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) have unspecified attitudes towards regulation, undefined regulatory powers and scope, and a lack of legal and practical jurisprudence to support them. The European Commission introduced a Markets in Crypto Assets Act (MiCA) in September 2020 to ensure that the EU's legislative services are adapted to the digital age, with the aim of proposing a comprehensive and harmonized regulatory policy for crypto asset markets.

It can be seen that while each jurisdiction has emphasized the development and possible risks and impacts of the digital asset space, the pace of their regulatory development has varied. By analysing the regulatory requirements in the field of digital assets, their consistent regulatory focus involves AML, CFT, KYC, KYT, Travel Rule and cybersecurity and other related areas, and the establishment of regulatory rules in these key areas can effectively reduce the risks of money laundering, terrorist financing, fraud and hacking.

In the face of the intricate global regulatory situation, what digital asset management organizations need to do is to cultivate their internal skills, actively embrace regulatory compliance, build their compliance framework based on the industry's compliance best practices, and tailor it appropriately according to the differences in various jurisdictions in order to adapt to the regulatory requirements of each place, which is the most optimal path to realize the rapid global expansion of the digital asset business in a compliant manner.

3.4.2 THE STORY: ACTIVELY EMBRACING COMPLIANCE REGULATION AND WINNING A HEAD START IN BUSINESS DEVELOPMENT

Amber Group is an active embracer and advocate of regulatory compliance. From the outset, we have established a comprehensive compliance framework based on the FATF anti-money laundering and counter-terrorist financing (AML/CFT) standards, licensing requirements in various jurisdictions, MSB (Money Services Business) requirements in the United States and Canada, International Standards Organization (ISO The Group has established a comprehensive compliance framework based on the information security and privacy management system requirements, and the AICPA SOC2 requirements, as well as the global regulatory requirements for digital assets, in order to prepare for the compliance challenges brought about by the development of the digital asset industry in a proactive manner.

On October 31, 2022, during the opening ceremony of Hong Kong FinTech Week, the Financial Services and Treasury Bureau (FSTB) of the HKSAR Government formally released the "Government Issues Policy Statement on Development of Virtual Assets in Hong Kong" (the "Declaration"). In 2023, the FSTB issued a consultation paper on the Proposed Regulatory Requirements for Virtual Asset Trading Platform Operators Licensed by the Securities and Futures Commission. An appendix to this paper outlines "Guidelines for Virtual Asset Trading Platform Operators."

The purpose of these documents is to establish a fair and transparent regulatory framework based on the principle of "same business, same risk, same rules." The framework and guidelines aim to clarify compliance requirements for operators of virtual asset trading platforms in Hong Kong. Additionally, the guidelines seek to provide direction for virtual asset service providers wishing to develop compliantly in the market.

This is a bright light for virtual asset service providers who intend to develop in a compliant manner.

Confidence in security and compliance solutions comes from long-term compliance practices and experience. The following is an introduction to the total solution for security and compliance applicable to digital asset management companies.

3.4.3 INDUSTRY SECURITY AND COMPLIANCE SOLUTIONS PRACTICES

A digital asset management company's security and compliance solution should consist of an information security and data privacy governance system and a digital asset compliance system. The two systems are integrated and supported by each other. The compliance requirements are implemented through technical, managerial, organizational and operational means, and the effectiveness of the system is ensured through regular external and independent third-party audits, certifications, and assurances.

3.4.3.1 INFORMATION SECURITY AND DATA PRIVACY GOVERNANCE SYSTEM

The Information Security and Data Privacy Governance System is a set of standards based on ISO/IEC 27001:2013 ("ISO 27001"), ISO/IEC 27701:2019 ("ISO 27701") and ISO/ IEC 29151:2017 ("ISO 29151"), incorporating AICPA SOC2, NIST Cyber Security Framework, NIST Privacy Framework, PCI DSS, Digital Asset License Security requirements of various jurisdictions.

The governance system combines the best security and privacy requirements of standards and forensic guidelines. The entire system covers the key areas of Identify, Protect, Detect, Respond, and Recover in cybersecurity and is continuously improved through the PDCA methodology of Plan-Do-Check-Act. The PDCA methodology of Plan-Do-Check-Act is used for continuous improvement. The following figure shows the IPDRR (Identification, Protection, Detection, Response and Recovery) based cyber security protection domain:

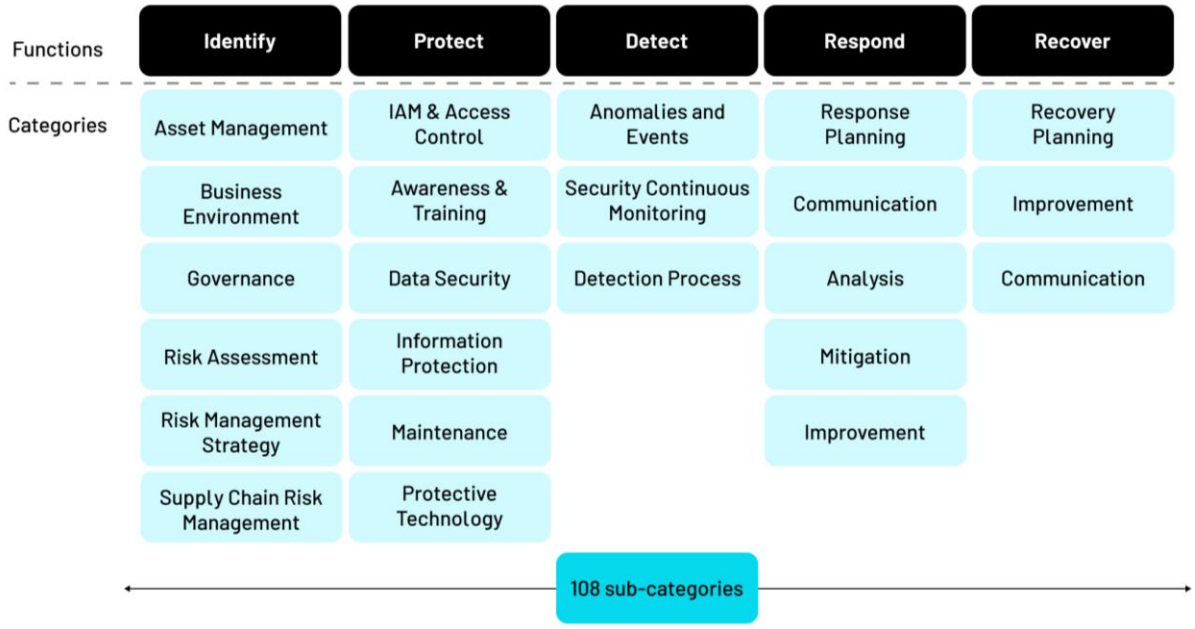

Figure: IPDRR Cybersecurity Lifecycle

Privacy is a crucial component of digital asset management company brand values. These companies should fully respect user privacy, maintain high levels of privacy transparency, and establish and operate sound organizational and technical controls to achieve end-to-end privacy protection. Companies can use a Data Security and Privacy Protection Framework based on relevant standards such as NIST Privacy Framework, ISO 27701, ISO 29151, and SOC 2.

By establishing five privacy management domains - Identify, Govern, Control, Communicate, and Protect (IGCCP) - based on the requirements of the EU GDPR privacy Act, digital asset management companies can tailor their privacy framework to meet data privacy regulatory compliance requirements worldwide. The privacy framework fully recognizes privacy laws and regulations in jurisdictions around the world.

The figure below shows the IGCCP-based data privacy protection domains:

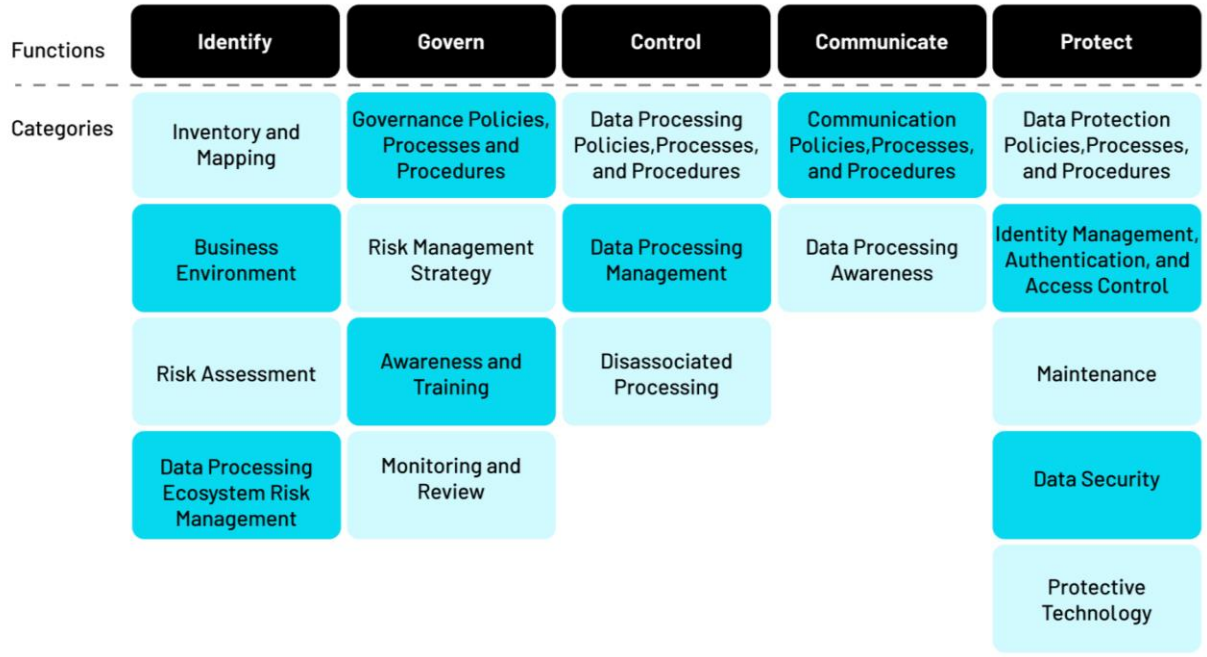

Figure: IGCCP Privacy Framework

3.4.3.1.1 INFORMATION SECURITY AND PRIVACY ORGANIZATIONAL STRUCTURE, RESPONSIBILITIES AND OPERATIONAL MECHANISMS

A robust information security and privacy organizational structure, along with clear responsibilities and operational mechanisms, is fundamental to ensuring that a digital asset management organization executes its information security and privacy work effectively.

Digital asset management companies can use the organizational structure design guidelines of IT governance and security and privacy standards, such as COBIT 5.0, ISO 27001, and ISO 27701, as a reference for their information security and privacy organizational structure. By establishing a four-tiered operational mechanism of decision-making, management, execution, and oversight through reasonable hierarchical setups and division of responsibilities, it is possible to achieve a structure characterized by reasonable division of labour, clear responsibilities, mutual checks and balances, and clear reporting relationships.

This structure fully reflects the comprehensiveness, compliance, sophistication, operability, and audit independence of the governance framework.

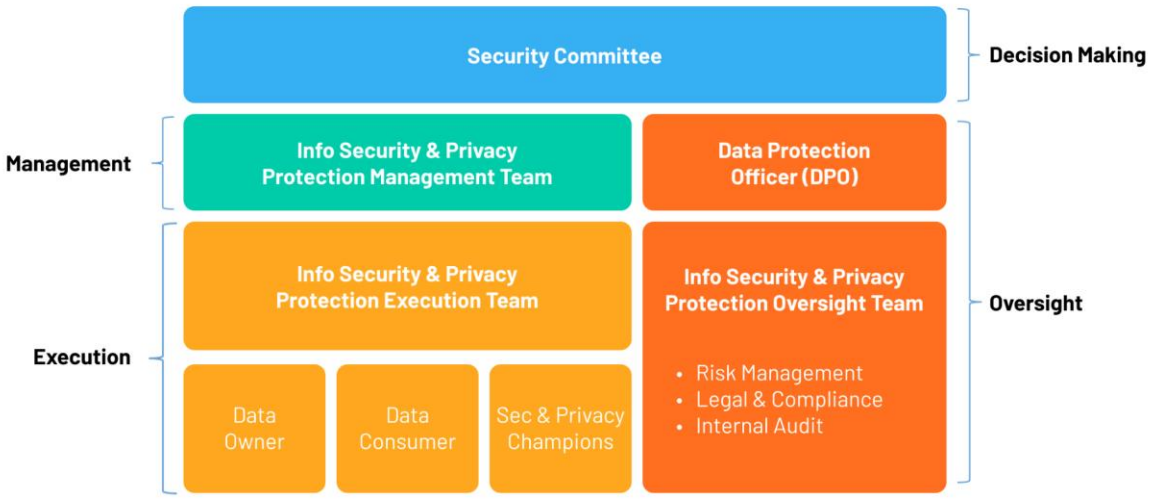

Figure: Information Security and Privacy Organizational Structure

- **Security Committee:** The Security Committee serves as the decision-making and deliberation body for planning and managing the Company's information security and privacy protection. It unifies the planning and management of organizations and personnel related to information security and privacy. The committee promotes the Company's information security and privacy protection by authorizing appropriate measures, reasonably allocating resources, and strengthening communication both internally and with other organizations. In addition, the Security Committee provides necessary security education and training to employees to ensure they possess the required competencies. It evaluates the effectiveness of measures taken and ensures that relevant personnel understand the importance of their activities and how they contribute to achieving

information security and privacy management policies and objectives. Through these efforts, the Security Committee contributes to realizing the Company's information security and privacy management policies and objectives.

- Information Security and Privacy Protection Management Team: The Information Security and Privacy Protection Management Team is responsible for constructing and operating the Company's information security and privacy protection policies, systems, and mechanisms in accordance with the strategic decisions of the Security Committee. They complete the daily communication, coordination, and management of information security and privacy protection.
- Information Security and Privacy Protection Execution Team:
    - The Information Security and Privacy Protection Management Team is comprised of several functional groups, including the Information Security Department, Data Owners, Data Consumers, and Information Security & Privacy Champions. Each group is responsible for implementing specific information security and privacy construction and operation work.
    - The data owner is the primary person responsible for the security and privacy of relevant data within the scope of business management. The data consumer is the person who uses the data and is responsible for complying with requirements related to data security and privacy protection.
    - Meanwhile, the Information Security & Privacy Champion is a cross-departmental coordinator and uploading functionary. They act as a communication bridge between the business department and the Information Security Department, assisting the latter in implementing information security and privacy control measures.
- Data Protection Officer: The Data Protection Officer is responsible for overseeing the company's compliance with data protection regulations and reporting independently to the Company's top management on its personal data and privacy protection efforts. They also act as a communication channel and point of contact between data subjects and supervisory authorities, handling complaints and suggestions from data subjects, dealing with supervisory inspections and assessments by supervisory authorities, providing advice on data protection impact assessments and data protection measures, and notifying supervisory authorities and data subjects in the event of a personal data breach.
- Information Security and Privacy Oversight Team: The Information Security and Privacy Oversight Team consists of risk management, legal affairs and compliance, and internal audit functions. They are responsible for independently auditing, supervising, and evaluating the management and implementation of data security and privacy protection strategies, management mechanisms, and controls at the executive levels of the organization to verify their effectiveness and compliance. This team reports independently to the Company's top management on their findings and recommendations.

In addition to the information security and privacy organizational structure design described above, it is essential to design a RACI matrix for core information security and privacy work to better

implement personnel responsibilities. A clear responsibility matrix and RACI matrix defining the roles of Responsible, Accountable, Consulted, and Informed for each privacy work area ensures effective responsibility implementation.

Through the design of these mechanisms, Digital Asset Management institutions can synchronize high-risk information security and privacy issues in a timely and accurate manner. They can quickly coordinate the implementation and rectification of relevant security risks with the cooperation of various business departments, product development departments, and functional departments, significantly enhancing the speed of iteration in achieving steady and continuous growth in cybersecurity maturity.

3.4.3.1.2 APPROACH TO BUILDING A GOVERNANCE SYSTEM FOR CROSS-STANDARD CONVERGENCE

To adapt to the rapidly evolving Web3 and digital asset era, an information security and privacy governance system should have stability, flexibility, system compatibility, and scalability. The principles, methodologies, and control domains of global information security and privacy governance system standards and norms are essentially the same, with differences only in specific fields' alignment methods with these standards. Therefore, each enterprise can refer to international standards and best practice frameworks to establish a solid foundation tailored to industry and enterprise-specific circumstances, which is the industry's best practice.

In the course of information security and privacy governance, organizations must continue to identify and integrate new security and privacy standard requirements and industry regulations to ensure they can integrate, adapt, and extend their control requirements on top of a solid foundation tailored to their organization's real-world situation.

For digital asset management companies, the recommended approach is to build, integrate, and validate methods to achieve a governance system that converges across standards.

- Construction: Build a solid base for the governance system based on ISO's information security and privacy management requirements, NIST CSF and PRF frameworks, making the information security and privacy governance system naturally compliant with international standards and best practices, providing a foundation for continuously integrating additional digital asset security requirements.
- Integration: Continuously identify the security requirements of digital asset licenses in the jurisdictions where the main business is conducted, as well as their differences and characteristics, and integrate them into the existing governance system. For example, Hong Kong, Singapore, and Japan have clear security and privacy requirements in their digital asset service licenses.
- Validation: Validation refers to independent verification of the effectiveness of the design and operation of the information security and privacy governance system by utilizing independent certification, attestation, assessment, and auditing services from external

third-party authoritative organizations, including but not limited to AICPA SOC2 Attestation Guidelines, ISO Security and Privacy Certification, and NIST Maturity Assessment.

3.4.3.1.3 INTELLIGENT ROBOTIC PROCESS AUTOMATION (RPA) EMPOWERS PROCESSES TO RUN EFFECTIVELY

Robotic Process Automation (RPA) is an automated process management system with low code, low cost, high interaction, high business fit, and high connectivity. It can be connected with enterprise management systems to form a highly interactive organism. RPA can automatically execute tasks and activities, and through scripts, it can also realize automatic entry, automatic flow, and process interaction functions. Using drag-and-drop and building blocks, it enables fast and convenient configuration and process deployment, providing a highly efficient flow channel for various enterprise processes.

Without an automated flow platform to support them, implementing information security and privacy policies, procedures, and guidelines may prove challenging. However, by automating the application, flow, and approval of key IT and security processes using intelligent RPA, intelligent correlation can be realized across multiple process groups.

Typical Case Presentation: Data Security Governance Based on Data Owner and Data Security Level Labelling

A typical case presentation is Data Security Governance based on data owner and data security level labelling. The foundation of data security governance is defining data owners and data levels so that different security controls can be set in place. Traditional practices of defining data owners and classification on paper are neither accurate nor relevant to automated processes as time passes.

With RPA, data owners who have been identified through data security governance are entered into the CMDB database. This gets updated throughout the database creation process, and changes occur when the database is taken offline or migrated, thus achieving closed-loop management of data owners throughout its lifecycle. At the same time, the data security classification label defined through the data discovery tool can be opened through API.

By interfacing with the CMDB database and data discovery tools, RPA can synchronize the receipt of the latest data in a timely manner. In each data process, RPA can dynamically generate the approver node of each data process based on the information of the data owner. It can also determine whether additional security control measures are required based on the data security level. Currently, this mechanism has been applied to many data-related processes, including database creation, data change, database offline, database migration, data usage export, data sharing, and data permission approval.

3.4.3.1.4 PRIVACY BY DESIGN-BASED PRIVACY GOVERNANCE APPROACH

Privacy by Design has developed a comprehensive set of theoretical foundations, including Privacy by Design Strategies, Privacy by Design Patterns, and the corresponding Dark Strategies and Dark Patterns. Prof. Ann Cavoukian from Ontario, Canada, originated the Privacy by Design theory in the 1990s by proposing seven basic principles of Privacy by Design, which serve as a foundation for subsequent development of Privacy by Design theory. These principles provide generalized guiding principles for privacy-protecting systems. The concepts related to Privacy by Design have been recognized by national regulators and international organizations such as the EU's GDPR Article 25 and the International Standards Organization (ISO).

In 2023, the International Standards Organization (ISO) published "ISO TR 31700-1-2023 Consumer protection — Privacy by design for consumer goods and services Part 1: High-level requirements" and "ISO TR 31700-2-2023, "Consumer protection — Privacy by design for consumer goods and services Part 2: Use Cases" as the PbD standard for the first time. This provides guidance for industry players on implementing strong privacy practices from the outset to better protect consumer data.

However, few companies have been able to truly implement these principles due to their abstractness. Therefore, the industry has been committed to concretizing them into a set of methodologies that can guide actual research and development while addressing different privacy needs. This is called Privacy Engineering, a specialized discipline of systems engineering focused on avoiding unacceptable privacy consequences when processing personally identifiable information. It integrates the need for privacy protection into the software development lifecycle and organizational and technical management processes, and is a result-oriented process supported by sufficient system implementation evidence.

Privacy Strategies are the implementation strategy mechanism of privacy engineering that solve actual risks. According to ISO/IEC TR 27550 Information Technology - Security Techniques - Privacy Engineering for System Lifecycle Processes, mainstream strategies include 8 types and 26 means, with four data protection-oriented and four process protection-oriented policy types. Privacy Design Pattern is the reusable design pattern based on privacy strategies, while the opposite of privacy strategies and privacy design patterns are called Privacy Dark Strategies and Privacy Dark Patterns.

Integrating Privacy by Design and Privacy Engineering into product and service design and development allows for a logical architectural rearrangement of Privacy by Design, Privacy

Engineering, Privacy Policies, and Privacy Patterns, as well as their opposites, Dark Policies and Dark Patterns. This facilitates better articulation of correlations between them.

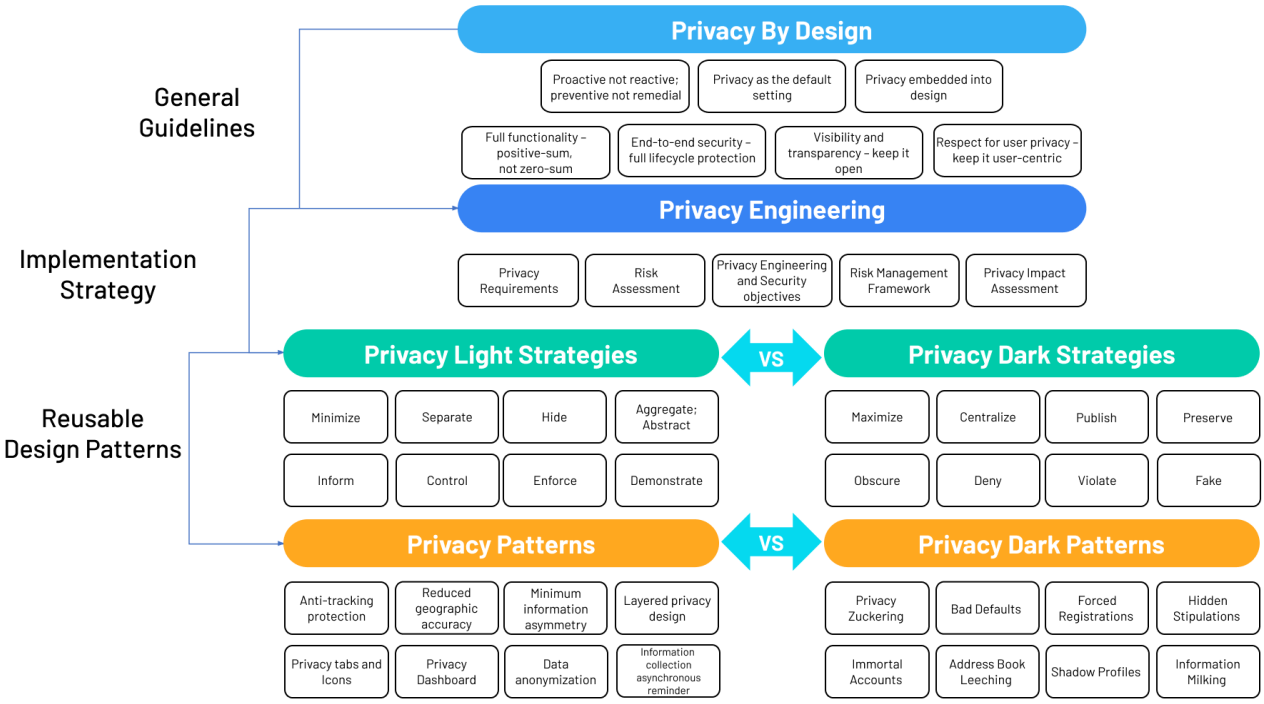

Figure: Logical Architecture of Privacy by Design Theory

Amber Group involves dedicated privacy experts in every stage of its product development process, from requirements design to impact analysis of privacy needs and risks. This ensures that our products are designed with strong privacy protections in mind, and that security technology tools such as zero trust, authentication, access control, data encryption, pseudonymization, auditing, and other security tools are implemented from the outset

Digital asset management companies can establish a Privacy Program Management Platform that clearly identifies and documents all data collection, processing activities, and data mapping. This platform can be used to construct automated privacy notification management, consent management, cookies management, data subject access right management, data breach response

management, and other measures to provide users with simple and convenient privacy management capabilities.

Information security and privacy are continuous improvement processes, and it is essential to continually track the latest privacy laws, regulations, and innovative privacy technologies to improve privacy maturity and provide customers with higher levels of privacy protection.

3.4.3.1.4.1 PRIVACY TECH PLATFORMS HELP INCREASE PRIVACY TRANSPARENCY

The privacy protection industry generally adopts PrivacyTech's one-stop privacy compliance solution, which effectively and deeply integrates with organizations' privacy engineering [18][19]. This provides strong methodology and technical capability support for enterprises that must comply with privacy data requirements.

The solution is divided into Planning, Construction, Integration, Validation, and Operation phases in privacy engineering practice. Each phase is compatible with the mainstream DevSecOps framework of cybersecurity and automated with advanced privacy technologies. Thus, privacy protection can be embedded into the enterprise R&D process framework in the smallest and most effective way, reducing resistance during the implementation of privacy protection.

Amber Group utilizes the industry's leading privacy management platform to build a privacy technology toolchain in the enterprise R&D process through Privacy by Design principles and privacy engineering practices. This provides digital asset management companies with wealth management platforms with privacy technology tools, including data discovery, categorization, mapping, consent management, privacy impact assessment, data subject rights response, cookie management, SDK permission scanning, vendor due diligence, privacy preference center, privacy and security incident management, and more.

By implementing a privacy management platform, organizations can automate numerous privacy processes and embed them directly into their workflows. This significantly reduces legal risks to privacy while strengthening protections for user and consumer data rights. Automated privacy processes enhance transparency for individuals and boost satisfaction through robust yet seamless privacy safeguards. The platform integrates privacy directly into operational procedures to help ensure ongoing compliance.

The following describes the practice of each phase of privacy engineering:

3.4.3.1.4.2 PLANNING PHASE OF THE PRIVACY ENGINEERING

The planning stage is mainly through the organization structure, personnel responsibilities, system processes, technology tools and knowledge management, etc. Planning and designing is the basic work of privacy engineering.

Amber Group has a comprehensive approach to information security and privacy governance, which encompasses Organizational Structure, Personnel Responsibilities, Policies and Procedures, Technology Tools, and Knowledge Management.

1) Organizational Structure: Amber Group 's information security and privacy organizational structure draws on IT governance and security and privacy standards, such as COBIT 5.0, ISO 27001, and ISO 27701. It establishes a four-tiered operation mechanism of decision-making, management, execution, and supervision through reasonable hierarchical setups and delineation of responsibilities, characterized by a reasonable division of labour, clear responsibilities, mutual checks and balances, and clear reporting relationships.
2) Personnel Responsibilities: The structure includes the Security Committee, the Information Security and Privacy Protection Management Group, the Information Security and Privacy Protection Execution Team (including Information Security and Privacy Department, Data Owners, Data Consumers, and Information Security & Privacy Champion), the Data Protection Officer, and the Information Security and Privacy Oversight Team. Establishing a clear responsibility matrix and RACI matrix enables clear definitions of roles that are responsible, accountable, approved, consulted, and informed for each privacy work area.
3) Policies & Procedures: Amber Group focuses on "standardization" in constructing information security and privacy policies and procedures. Its governance system is designed to have stability, flexibility, system compatibility, and scalability, enabling it to quickly adapt to regulatory policies and privacy standards and norms. The global information security and privacy governance system is standardized, and each enterprise can refer to international standards and best practices frameworks to establish a solid foundation tailored to industry and enterprise-specific circumstances.
4) Technology Tools: Amber Group has adopted the industry's leading privacy management platform to establish a privacy technology tool chain in the enterprise R&D process. This provides a range of privacy technology capabilities, including data discovery, classification, mapping, consent management, impact assessment, data subject rights response, cookie management, SDK permission scanning, privacy and security incident management, vendor due diligence, and privacy preference center. With the application and deployment of the privacy management platform within the organization, numerous privacy processes are embedded into the organization's processes through automated processes, reducing privacy legal risks and enhancing privacy transparency and user satisfaction.
5) Knowledge Management: Amber Group recognizes the importance of knowledge transfer and deposition in achieving close and effective cooperation among different departments. It has

introduced a database of data privacy compliance laws and regulations to monitor global changes in data compliance and provide interpretation and translation services. In addition, an enterprise-level knowledge base platform records privacy design strategies, patterns, user interface design prototype diagrams, impact influence assessments, data processing activity descriptions, data mappings, and other experiences related to the company's digital asset business products for use in establishing reusable privacy design patterns.

3.4.3.1.4.3 CONSTRUCTION PHASE OF PRIVACY ENGINEERING

The privacy engineering construction phase takes place during the product requirements and design definition phase, initiated jointly by business personnel and product managers. When new product requirements are created on the project collaboration management system, trained product managers make a preliminary questionnaire analysis based on the "Privacy Threshold Analysis" defined in the standard "ISO/IEC 29134:2017 Information Technology - Security Technologies - Guidance for Privacy Impact Assessment." If a product requirement involves processing personal data that meets any of several conditions, it's subject to privacy compliance-related requirements and needs to proceed to the next step of the privacy impact assessment.

The Privacy Impact Assessment (PIA) is done by the privacy technology team in conjunction with the product manager and includes work such as combing the Data Inventory, creating a Record of Data Processing Activity (RoPA), Data Mapping, and Data Flow Diagram. The related records will be created, and if a DPIA must be initiated in relation to the conditions defined in the EU GDPR, the report will be completed in parallel with the DPIA requirements of GDPR and will be ready for review. If there's no unacceptably high risk, the design phase for product privacy will be formalized. Still, if the results of the DPIA indicate high risk, further assessment of mitigating measures or opting out of the data processing activity will be required on a case-by-case basis.

During the privacy design phase, the privacy technology team builds a privacy design for a specific business based on a series of analytical process documents created by the privacy impact assessment. The privacy design is divided into an initial build and an iterative update.

The initial construction of the product's privacy design includes privacy notification and interactive interface layering design, consent record collection, special category data collection separate consent/explicit consent design, privacy policy update notification, cookies and SDK identification and permission collection design, cookies banner design, data subject access request interface and interfacing, data display desensitization, log output desensitization, database design (including data segregation), data localization storage design, database field encryption, data retention timestamp marking, data periodic deletion script design, and privacy settings preference center design.

Iterative updates to the product focus on changes to the product requirements' content, including identifying personal data based on new collection, updating the privacy policy, adding a point of collection for recording consent for privacy data, etc.

Records of the above privacy design will be documented through the Project Collaboration Management System (PCMS), which maintains relevant records of evidence to meet compliance evidence retention requirements.

3.4.3.1.4.4 INTEGRATION PHASE OF THE PRIVACY ENGINEERING

The privacy engineering integration phase consists of the various designs from the privacy build phase through the steps of privacy notification and interaction interface development, product and database development and privacy management platform configuration and integration.

1) Privacy notification and interactive interface development
   Amber Group works with product managers on the layering of privacy notifications and interactions to strike a good balance between business convenience and privacy protection to meet the "positive-sum not zero-sum" principle of Privacy by Design. A privacy notification can be effectively communicated by adopting a combination of privacy notifications to achieve an optimal solution for the user interface. This can range from static privacy notification text, enhanced notifications, instant alerts, separate consent, privacy icons and symbols, and notifications of privacy policy updates.
2) Product, database development and privacy management platform configuration
   Digital Asset Management Company works primarily with developers and DBAs in the actual development and implementation of the product and database development process. The Privacy Technology team accomplishes the following tasks:
   - Data collection point implementation: Determine the consent record collection technology for Web, App and applet, you can choose to embed the privacy management platform's JavaScript, SDK, or utilize the privacy management platform's API for the push of the consent record, so as to achieve the effective retention of the consent record;
   - Mobile App Compliance Management SDK Integration: Mobile App Compliance Management SDK Integration for Privacy Management Platform, the process requires configuring the interface, text, colour, Logo of the App pop-up window and Privacy Preference Center, and configuring the geolocation rules (PIPA, GDPR, CCPA, etc.) on the Privacy Management Platform. After the configuration is exported from the SDK, it is handed over to the developer for integration into the app;
   - Data Subject Rights Response Implementation Integration: Data Subject Rights Response requires the configuration of geographic location rules, data subject authentication configuration, response process guidelines, response workflow within the enterprise, and other related configurations on the privacy management platform. The final data subject rights response page will be integrated by the developer at the bottom of the product homepage and embedded in the contact section of the privacy policy by hyperlink;
   - Data table design: By establishing a user-cantered data table as a centralized database for user data, and by using a unique identifier as a foreign key between multiple database tables for connecting to other application systems and modules, it reduces

the risk of dispersed storage of sensitive personal data in multiple database tables, and also reduces the difficulty of privacy data management;

- Personal data timestamp marking: According to data classification and grading, financial transaction data will generally be stored in the form of UID + transaction data, which has a more independent database table structure that can facilitate data categorization for disposal. In terms of timestamp, the transaction data should be marked with a timestamp from the time it is generated, and the timestamps of the database tables should be polled periodically to generate tasks for data deletion or anonymization for subsequent processing;
- Data Field Encryption in Database: Identify personal data fields that require data field encryption and use the cloud provider's application encryption SDK and KMS to complete the data field encryption work;
- Data display desensitization: According to the enterprise desensitization standard, complete the desensitization of sensitive personal data display in the front-end of the product and the desensitization of log data in the back-end.

3.4.3.1.4.5 PRIVACY ENGINEERING VALIDATION PHASE

The privacy engineering validation phase focuses on validating the compliance of the specific implementation of the design and development, and checking whether the privacy requirements are met. The main work includes Web Cookies scanning, App and SDK data collection and permission scanning, and privacy function user acceptance testing.

- Web Cookies Scanning: A privacy management platform is used to scan the actual cookies deployed on web pages to verify that the cookies are consistent with the design. Cookies are categorized after the scan is complete, and all but the strictly necessary categories of cookies should have the user's explicit consent to place and collect data. The results of these scans need to be synchronized and configured into the Cookies banner to meet Cookies compliance requirements;
- App and SDK Data Collection and Permission Scanning: Adopting the method of App detection tool + manual service, we conduct compliance testing on the type, scope, frequency and necessity of data collection by App and SDK, and cross verify the actual test results with the privacy policy and various list appendices, and update the corresponding documents;
- User Acceptance Test for Privacy Functions: Mainly conduct user acceptance tests for various privacy notifications, privacy policies, privacy interface interactions, text accuracy, hyperlink validity, and process validity.

3.4.3.1.4.6 OPERATIONAL PHASE OF THE PRIVACY ENGINEERING

The operational phase of privacy engineering focuses on maintaining existing privacy engineering measures and processes, including dynamic tracking of data compliance requirements, data discovery and categorization and classification, data subject rights response, data leakage prevention operations, personal data leakage response, supplier privacy risk management, and other related tasks.

- Dynamic tracking of data compliance requirements: Identify the latest status of data laws, regulations and standards in the scope of business by subscribing to the latest dynamic messages from the database of data privacy compliance laws and regulations and consider the need to internalize compliance requirements;
- Data discovery and classification: Regular scanning of all databases in the enterprise through data mapping tools to identify whether there are any changes in personal data or new databases added to bypass the data process, which may result in the risk of loss of control over the scope of personal data. Data discovery and classification can provide basic data support for Data Inventory (DI) and Record of Data Processing Activities (RoPA);
- Data Subject Rights Response: Regularly monitor the DSAR page status of DPO mailboxes and privacy management platforms, and if there is a data request, respond to the data rights in accordance with the internal response process of the organization;
- Data Leakage Prevention Operations: Amber Group has established a set of overall data leakage prevention solutions based on Cloud Native, SASE, Zero Trust, and UEBA, which can perform actions such as monitoring, blocking, isolation, and approval of outgoing personal data to reduce the risk of personal data leakage;
- Personal Data Breach Response: Amber Group conducts an annual data breach emergency response drill, which is jointly implemented by legal, security, privacy, compliance, PR, product, business, sales, and human resources departments to simulate the corporate response mechanism under various privacy breach scenarios. In the unfortunate event of a data breach, a data breach investigation will be initiated to remediate the incident, while public opinion will be well monitored, and users and regulators will be notified in accordance with compliance requirements. Finally, we will summarize the data breach incident and optimize the related process mechanism;
- Supplier Privacy Risk Management: In the process of enterprise supply chain security management, there usually exist management nodes such as project evaluation, supplier due diligence, product and service procurement, contract signing, supplier performance evaluation, and contract termination, etc., and privacy protection can be realized by embedding the control process in each node. Amber Group adopts intelligent Robotic Process Automation (RPA) to control most of the supplier privacy risk management, and embedding process choke points into various processes can achieve the best privacy risk management results.

3.4.3.2 DIGITAL ASSET COMPLIANCE SYSTEM

The Digital Asset Compliance System is a set of systems and processes established to ensure that digital asset transactions and use comply with laws, regulations and compliance requirements such as Anti-Money Laundering (AML).

The main objective of the Digital Asset Compliance System is to promote transparency, compliance and security in the digital asset industry and to prevent money laundering, illicit financial flows, terrorist financing and other illegal activities.

3.4.3.2.1 KNOW YOUR CUSTOMER - KYC

By verifying a customer's identity, address and company background, financial institutions are able to better understand their customers and assess the risks of doing business with them. This helps to maintain the stability of the financial system and ensure compliance.

- Proof of identity: Clients are asked to submit scanned copies of valid documents to confirm their identity and personal details. Proof of identity documents issued by the country/region, such as passports, identity cards or driver's licenses, are usually requested. These documents are verified and compared with the information provided by the customer;
- Sanctions: Ongoing list scanning through industry sanctions list vendors to motivate violators to change their behaviour while protecting the stability and security of the global financial system;
- Proof of address: In addition to proof of identity, clients are required to provide valid proof-of-address documents to verify their residential address. This may include documents such as bank statements, utility bills, resident registration certificates or rental contracts. We will use these documents to confirm the client's actual place of residence;
- Company structure: For corporate clients, an understanding of the company's structure and business model is required. We will ask companies to provide their articles of association, incorporation documents, shareholder structure, details of directors and senior management, etc. This helps us to understand the background and operations of the company and assess the risk of entering into a business relationship with it;
- Company-related directors: Corporate clients are asked to provide details of directors and officers who are related to the company. This information may include the director's name, address, nationality, position, educational background and professional experience. We conduct due diligence on these individuals to ensure their legitimacy and credibility.

The KYC process involves not only the verification of a customer's identity and background, but also a risk assessment of the customer. The risk level of the customer is assessed based on factors such as their business activities, compliance standards in the country/region of residence, and suspicious behaviour of the customer. This helps determine whether more stringent monitoring and due diligence is required. We also continuously monitor our customers' risk levels to ensure that their information is accurate and timely. If there is a change in a customer's risk profile or suspicious activity, financial institutions should take appropriate measures to

investigate and report to the relevant authorities. KYC becomes more complex when it comes to cross-border business. Different countries/regions may have different KYC requirements and regulatory standards.

Amber Group has been working to form geographic compliance teams to understand and comply with relevant country/territory regulations and to ensure that cross-border customer identification and due diligence meets the requirements of the respective jurisdictions.

3.4.3.2.2 AML, KYT AND TRANSACTION MONITORING

KYT (Know Your Transactions) is another concept related to KYC (Know Your Customer), which focuses on monitoring and understanding a customer's trading activities in order to identify risks that may involve money laundering, fraud or other illegal activities. This can be accomplished through early warning and historical backtracking using the industry's top KYT detection tools:

- **Transaction monitoring:** The use of automated systems to monitor customer transaction activity. These systems can analyse various aspects of transactions, such as amounts, frequency, countries/regions involved, etc., to look for unusual or suspicious patterns. For example, if a customer makes large transfers or transactions involving high-risk countries/regions within a short period of time, this may be of concern to the system;
- **Risk Analysis:** KYT uses risk analysis models to assess the potential risk of a transaction. These models combine several factors, such as the customer's risk level, the type and amount of the transaction, and the background of the counterparty, to determine a transaction's risk score. Transactions with high risk scores will require further review and investigation;
- **Suspicious Transaction Reports:** If a financial institution discovers suspicious transaction activity, depending on the laws and regulations of the country in which the financial institution is located, we will, at our discretion, submit a Suspicious Transaction Report (STR) to the appropriate regulatory agency. the STR contains detailed transaction information and a description of the suspicious activity to allow the regulatory agency to conduct further investigations and processing;
- **Data analytics:** KYT uses big data analytics to process and analyse large amounts of transaction data. By mining and analysing this data, financial institutions can uncover hidden patterns, correlations and anomalies to better identify potential risks. This may involve the use of machine learning algorithms, artificial intelligence and data mining techniques.

Through KYT, we are able to better monitor and manage our clients' trading activities, and identify and respond to potential risks in a timely manner. This helps prevent money laundering, terrorist financing and other illegal activities, while protecting the security and stability of the digital asset system.

3.4.3.2.3 INDUSTRY SELF-REGULATION OF TRAVEL RULES (TRAVEL RULE)

The Travel Rule is a requirement developed by the International Financial Action Task Force (FATF) for Virtual Asset Service Providers (VASPs). The rule requires VASPs to share identifying information about senders and receivers when making virtual asset transfers.

Amber Group is committed to promoting the implementation of Travel Rule to ensure the compliance and security of virtual asset transactions between counterparties and to reduce the risk of money laundering and illicit money activities. This helps to enhance the credibility of the entire virtual assets industry and promotes its interoperability with the traditional financial system.

3.4.3.3 DIGITAL ASSET SECURITY AUDIT

Blockchain is one of the most promising technological advancements in recent years, and data asset management companies need to understand the risks associated with blockchain in the early stages of its business and technology and consider taking control measures to address. In order for data asset management companies to implement, govern, secure, audit, and safeguard blockchain correctly and securely, Ankura suggest that data asset management companies refer to the Information Security and Data Privacy Governance Frameworks (ISO/IEC 27001:2013 ("ISO 27001"); ISO/IEC 27701:2019 ("ISO 27701"); ISO/IEC 29151:2017 ("ISO 29151"), AICPA SOC2, NIST Cyber Security Framework, NIST Privacy Framework, PCI DSS, etc.,) ISACA Blockchain Framework Audit Program [26] and regional privacy compliance requirements, and evaluate blockchain risks based on actual business processes, and timely implement relevant control measures for risk control.

3.4.3.3.1 AUDIT STRATEGY

Digital asset security audits provide management teams with an assessment of the blockchain technology control environment to indicate whether the design is sufficient and whether operations are effective. They identify any governance challenges and blockchain risks that may lead to reputational, legal, and/or significant financial impacts. Security audits also provide management teams with a comprehensive risk management perspective that considers both technical and non-technical factors.

Ankura suggests customizing audit methods and steps for different audit control items based on actual business situations and conducting regular security audits.

3.4.3.3.2 AUDIT TARGETS

Ankura suggests that digital asset management companies clearly define the audit targets when conducting blockchain audits with considerations of applicable framework requirements. The audit targets suggested to cover the following areas:

1) Governance
   The existing blockchain/distributed ledger technologies involve organization, policy, process related guidelines and requirements, as well as compliance with local regulations.
2) Infrastructure
   Any functionality or capability of a blockchain independent from the data transacting on the blockchain or among blockchains that ensures sufficient security, availability, processing integrity, confidentiality, and privacy. Establishing sufficient preventive measures to respond to threats and attacks.
3) Data Security
   Off-chain information stored and/or transmitted in a computer-readable format for transactions or interactions on the blockchain network, or data from a real source considered for commercial purposes from the blockchain network.
4) Privacy Protection
   Developing organizational, political, and technical measures based on privacy management standards in different countries and regions, combined with privacy management frameworks. Reviewing privacy management to ensure that users can control the collection and use of their data while protecting the security of sensitive information.
5) Key Management
   The management of public and private keys involved in the business process, as well as the design, generation, storage, transmission, and management of keys, to ensure the security, sustainability, and compliance of the entire process.
6) Smart Contracts
   Including impacted DLT networks, Oracle® calls and integrated code between blockchain recording of state and other transaction data.

In every field, the audit team needs to carefully review and assess various measures to identify potential security risks and compliance issues. The audit report should provide detailed

information, including problem description, risk level, and recommended remediation measures, to help the project team improve security and compliance capabilities. This audit process helps to ensure the credibility and user trust of digital assets.

3.4.3.4 CROSS-REGIONAL AND CROSS-PROFESSIONAL COOPERATION

Due to the decentralized and borderless nature of digital assets, many cases involve the flow and tracking of funds that have crossed multiple countries and regulatory regions. In such cases, regulatory requirements and regulations vary greatly from country to country, making it difficult for in-house resources to resolve complex and transnational issues on their own. As a result, global technology and legal consulting firms are taking an increasingly prominent role in such field.

The following details are noteworthy when it comes to cross-regional and cross-professional cooperation:

- Case Complexity: Case complexity increases significantly as digital asset transactions may involve laws of multiple countries, financial regulations, and privacy requirements. Cross-regional cooperation can assist in analysing and resolving legal issues under different jurisdictions.
- Global Resource Utilization: Global technology and legal consulting firms have specialized resources in every country, including legal experts, technical experts and regulatory affairs specialists. These resources can provide insights into country-specific regulations and policies and help organizations understand the diverse regulatory environment.
- Local Expert Collaboration: When working on multinational cases, it is important to collaborate with local experts. Cross-regional collaboration fosters close cooperation with local lawyers, regulators, and government agencies to ensure compliance with local regulations.
- Regulator Response: Global consulting firms can assist companies in developing cross-border compliance strategies to ensure transparent communication with local regulators and avoid unnecessary legal disputes and penalties.
- Information Sharing and Data Privacy: Information sharing and data privacy is one of the challenges in cross-regional collaboration. Business partners should ensure that applicable data privacy regulations are followed during information sharing to protect sensitive customer information.
- Technical Support: Cross-regional collaboration may involve technical challenges, such as blockchain analysis and digital evidence collection. Global technology consulting firms can provide technical support that can help track the flow of funds and evidence in cases.
- Legal Adaptability: The legal environment in different countries is constantly evolving, and organizations need to adapt their strategies to changes in a timely manner. A global consulting firm can provide sensitivity to legal changes and make timely adjustments.

In summary, cross-regional and cross-professional collaboration is critical in the digital asset industry. Business partners can provide companies with specialized resources, legal insights and

technical support on a global scale to assist them in dealing with diverse regulatory environments and complex case challenges. Such cooperation can help improve compliance and risk management for enterprises on a global scale.

IV. CONCLUSION

Cyber security, compliance, and risk management are essential elements in the digital asset industry. This content discusses the four main challenges faced by the digital asset industry and provides a series of effective solutions and practical cases to help enterprises and practitioners better cope with these challenges.

We need to focus on areas such as Web3 and blockchain security systems practice, digital asset business risk control framework, data security, and privacy protection framework. By drawing lessons from practical cases, we can ensure the security, compliance, and sustainable development of digital assets.

As the digital asset industry continues to develop, we must remain vigilant to new challenges and opportunities, actively promoting innovation and development in this field. By doing so, we can make contributions to the sustainability and stability of the financial system.

V. THOUGHTWORKS PERSPECTIVE

5.1 INSIGHTS INTO SECURITY, COMPLIANCE AND RISK CONTROL PRACTICES IN THE DIGITAL ASSET INDUSTRY

Throughout the world, the sweeping trend of the digital wave has been unstoppable, blockchain and artificial intelligence and other emerging digital technologies have given rise to a new type of digital economy, and governments and enterprises around the world are actively engaged in the emerging field of the digital economy, exploring ways to boost the economic development of science and technology, and enjoying the new dividends brought about by scientific and technological innovation.

In this era of economic growth driven by cutting-edge technology, the rise of digital assets has taken center stage like a shining star. Digital assets have been more than a decade since their birth, and the savage growth in the early stage has led to chaos in the industry, with one get-rich-quick myth attracting countless crypto-native players and speculators to pour into the market, but also zeroing out countless people's property in one cycle of rotation and hacking, a field where high yield and high risk coexist. No emerging financial sector has ever been able to rely on speculation for long-term development. An open, transparent, secure and stable regulatory environment is a prerequisite for an industry to thrive. Financial regulators in major economies around the world have begun to increase their efforts to regulate digital assets in recent years, and are committed to building a good regulatory framework, establishing a stable investment environment and creating a culture of compliance.

From Thoughtworks' long-term observation of the digital asset industry, we find that there are already quite a few enterprises that aspire to have a long-term vision in the digital asset field, and are actively building security, compliance and risk control systems that meet regulatory requirements. They are able to comprehensively utilize the security solutions of the Web3 industry and the global digital asset compliance concepts and methodologies, and enhance the enterprise's Through these technologies and management concepts, they are able to enhance the level of risk governance and equip enterprises with strong anti-risk resilience in the Web3 and digital asset sectors. Among them, Amber Group is an outstanding representative in this field. From the viewpoint of their digital asset security, compliance and risk control practice cases, they have achieved industry-leading levels in traditional security attack and defense confrontation, digital asset business security and risk control system, and digital asset security and compliance framework. In terms of Web3 security, it adopts the "Web3 Project Security Practice Requirements" developed by SlowMist, and utilizes the methodological framework of Web3 project life cycle security for security protection. Meanwhile, for project operational monitoring, the utilization of BlockSec's on-chain tracking and monitoring technology has enabled, which provides the industry with the best answer for on-chain security practice.

The establishment of a security system based on the project lifecycle is highly consistent with the technology philosophy advocated by Thoughtworks. "BizDevSecOps" represents a full-process

security and risk control methodology, which is a typical security methodology in the process of asset digitization, and can improve the transparency and efficiency of digital asset transactions, and establish a full-process security protection through the built-in security mechanism of the business. We observe that Amber Group has adopted the "Business Security Risk Management Methodology Based on Data and Financial Flows", "Privacy by Design Privacy Engineering Practices", and the "Web3 Project Lifecycle Integrated Chain Security Methodology" are all business-oriented security practices.

Furthermore, the integration of Artificial Intelligence (AI) with security in the realm of digital assets and Web3 has become a pivotal area of research for Thoughtworks. The ever-evolving landscape of AI technology holds immense potential and cannot be disregarded. Notably, the amalgamation of AI and security has yielded remarkable outcomes in anomaly detection, threat intelligence, intelligent security analysis, and automated security response. Alongside the ingenious on-chain analysis, other notable advancements such as SOAR & AI intelligent response and KYT intelligent data analysis, as showcased by Amber Group, BlockSec, and SlowMist, have captured our attention. These developments are indicative of wider industry trends and offer valuable insights to our readers.

5.2 DEFENSE IN DEPTH FOR DIGITAL ASSET SECURITY: THE BIZDEVSECOPS PROCESS

Asset digitization is the process of converting physical assets into digital form so that they can be managed, traded and utilized more efficiently. Through the use of various technologies and platforms, information about physical assets is converted into digital data and stored and transmitted in an electronically accessible form. Assets can include various forms of value carriers, such as currency, real estate, stocks, bonds, intellectual property, etc. The purpose of asset digitization is to increase the liquidity, visibility and operability of assets, making them easier to trade, transfer and manage.

Through asset digitization, information about physical assets can be accurately recorded, tracked and verified. This reduces the risk of information asymmetry and improves the transparency and efficiency of transactions. In addition, digitized assets can be better integrated with modern technologies and financial tools, such as smart contracts, blockchain and automated trading, to further optimize the process of asset management and trading.

Asset digitization has applications in many areas, including financial markets, real estate, art transactions and intellectual property management. It offers many potential benefits to all parties, including increased liquidity, reduced transaction costs, increased value of assets and convenience.

Undoubtedly, the process of asset digitization needs to rely on information technology to realize and replace the process of physical assets, this process will undoubtedly have a lot of problems and risks, for the security and compliance risks that are occurring in the future as well as those that may occur in the future, there is still a need for a sound quality process, so we believe that "BizDevSecOps" represents a typical form of full-process security and risk control approach in the

future process of asset digitization. Therefore, we believe that the "BizDevSecOps" approach to full-process security and risk control is a typical form of asset digitization in the future.

"BizDevSecOps" as a complete security built into the business development and operation process, and at the same time show the ability of the deep defense system state, in the process of "asset digitization", such a built-in security practice model still plays an important role. Thoughtworks has worked with several customers in this area, and these collaborations have reinforced our belief that BizDevSecOps, with its high degree of integration, will become a key platform for integrating security practices and a vehicle for implementation.

5.2.1 ADDRESSING FINTECH SECURITY THROUGH DIGITAL BUILT-IN SECURITY PRACTICES MEASURES

DevSecOps, the cultural movement we have seen consistently over the past five years to build security activities into the R&D process and increase automation, is becoming more mainstream as the DevOps culture builds. The responsibility of gatekeeping and caretaking by security testing is gradually being shared by activities such as continuous integration and automated security testing tools that bring higher frequency and shorter feedback cycles. This also allows developers to build a higher level of security awareness and skill.

A DevSecOps process typically consists of three phases:

- Security Plan/Demand Management/Design phase
- Secure Coding/Building/Testing/Automation phases
- Security Release/Monitoring/Operation Phase

Each of these stages encompasses a large number of security practices and the use of appropriate tools, and both fintech business owners and vendors involved in the construction of various types of digital systems may play a key role in the process and take responsibility for the delivery of value while being accountable for the services or products they provide, ultimately delivering digital assets securely to the investors and consumers of the financial business.

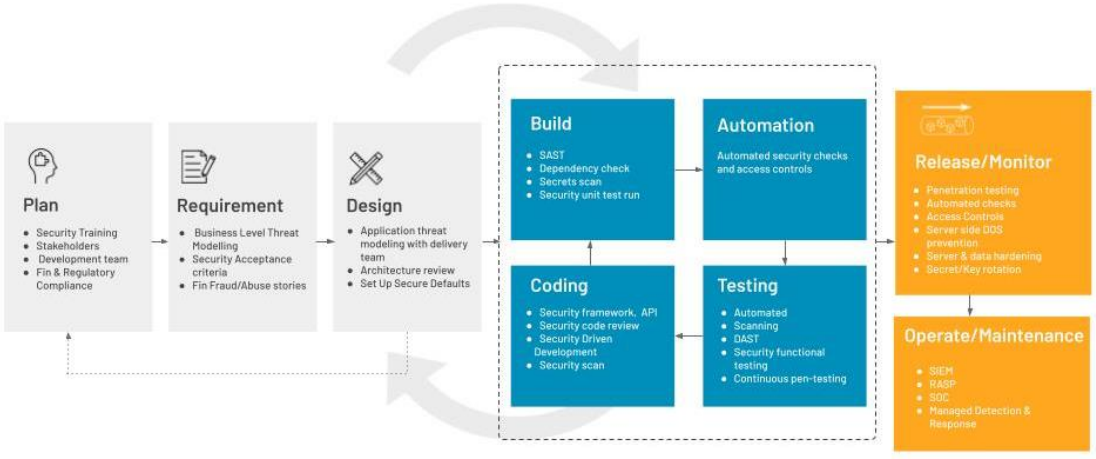

Figure: DevSecOps Security Development Lifecycle

In addition to this, a number of other levels of practices are built into various aspects of FinTech-type businesses along with the DevSecOps process. Here are some typical security practices related to digitization of financial assets, and they have probably penetrated most of the enterprises, serving as a complete defense-in-depth.

- Enhanced authentication: Implement multi-factor authentication (e.g. SMS authentication codes, hardware tokens, biometrics, etc.) to ensure the security of user identities. This can effectively prevent unauthorized access and identity theft;
- Data encryption technology: Strong encryption algorithms and protocols are used to encrypt digital assets, including during transmission and storage. This ensures the confidentiality and integrity of data and prevents unauthorized access and tampering;
- Security training and awareness-raising campaigns (e.g., Security Champion roles): Educate users and employees on best practices and potential threats to the security of digital assets through regular training and awareness-raising campaigns. Improve user and employee recognition of fraud, phishing attacks, and malware to reduce the risk of social engineering attacks;
- Blockchain technology applications: For application scenarios that require high security and transparency of digital assets, blockchain technology can be considered. Blockchain's distributed nature, non-tamperability and smart contract function can provide higher security and trustworthiness;
- Security Compliance and Regulatory Compliance: Comply with relevant regulations and compliance requirements, such as KYC (Know Your Customer) and AML (Anti-Money Laundering) requirements. Ensure that digital asset trading platforms and service providers are compliant with applicable regulations to protect users and assets.
- Continuous Governance, Improvement and Evolution: Keeping a close eye on the latest trends and threats in the field of digital asset security, continuously updating and improving security measures. Maintain cooperation with the security community and professional organizations to share experiences and best practices.

By using a combination of these digitization tools, the security of digital assets can be improved, potential risks can be mitigated, and the assets of users and businesses can be protected.

The recent emergence of the "BizDevSecOps" change goes even further, applying this technology-driven systematic thinking to the earlier stages of business design, which will greatly enhance the ability of business people to perceive and anticipate the security issues that accompany ongoing patterns and technological innovations.

5.2.2 TAKING OPERATIONAL SECURITY INTO ACCOUNT

As a link closely integrated with business value, business security, in the past, has been a high incidence of security incidents, how to more effectively identify the risks faced by digital assets at all stages, Thoughtworks believes that the following major sources of risk should be considered first:

- Social Responsibility and Goodwill Risk: As organizations become more digitized, the demands on the social responsibility level increase, and goodwill risk becomes a more vulnerable aspect to be infringed upon and combated. Business continuity issues that used to be caused by information leakage, data corruption, and loss of assets will be magnified in the digital asset space. Especially in the cryptocurrency industry, data corruption, loss and leakage mean direct asset loss.
- Fraud and Phishing: Cyber scams and phishing attacks are among the most common security threats in the digital asset space. Attackers may trick users into providing sensitive information or transferring digital assets through fake emails, social media messages or malicious websites;
- Hacking or APT: Hackers may exploit vulnerabilities or weaknesses to break into a digital asset's network or application. They may attempt to steal digital assets, tamper with transactions, disrupt services or gain access to user credentials;
- Malware: Malware (e.g., viruses, Trojans, and ransomware) can be used to steal digital assets, record sensitive information, or perform other malicious activities by infecting a user's device;
- Centralized Exchange and Source Risks: Centralized asset exchanges, as well as sources, as the primary platform for digital asset trading and the source of business data, still face more traditional security risks. These risks include hacking of exchanges and fiduciaries, leakage of internal privileges, and loss of assets due to system failures or process security breaches;
- Smart Contract Vulnerabilities: Smart contracts are automatically executed programs on blockchain-based digital asset platforms. Due to coding errors or design flaws, smart contracts may be vulnerable, resulting in stolen or unrecoverable assets;
- Social Engineering Attacks: Social engineering attacks gain sensitive information or access by exploiting human social workings and psychological deception. Attackers may trick users into revealing passwords, private keys, or other sensitive information through deception, impersonation, or entrapment;
- Regulatory Compliance Risks: The digital asset industry faces regulatory and compliance risks. Regulators may enact new regulations requiring digital asset trading platforms, wallet providers and other related entities to adhere to specific compliance standards or face possible fines or other legal consequences;
- Business Continuity: Organizations need to maintain business-critical operations and services in the face of various internal and external disruptions, disasters or emergencies. In the digital assets and finance space, business continuity is important because the

operation of financial transactions and digital assets is critical to the safe accessibility and tradability of assets for businesses and customers.

To address these security risks, users and organizations should adopt comprehensive security measures, such as using secure wallets and trading platforms, updating software regularly, monitoring and fixing 0day vulnerabilities in a timely manner, implementing strong passwords and multi-factor authentication, backing up data on a regular basis, staying vigilant to prevent fraudulent phishing, and raising awareness of security in environments including social and office. Also, choosing a trusted and compliant digital asset service provider is an important security decision.

In the security and risk control practices implemented by leading digital asset service providers, such as Amber Group, we have found that continuous monitoring, governance, self-examination and optimization of security practices and risk control tools, as well as the construction of a sound and efficient feedback mechanism, are crucial for "digital asset native" organizations.

In addition to this, we are seeing some new changes, as AI technology matures, the original process of relying on the experience of security experts for problem discovery and answering around business analytics is expected to be more automated in terms of identification and processing. We believe that the improved situational and contextual awareness brought about by means such as the introduction of LLM (Large Language Models) in digital systems could be the breaking point for the next generation of business and application security practices.

5.3 AISEC - SECURITY TECHNOLOGY TRENDS FOR SCALING DIGITAL ASSETS

Asset digitization is the process of converting traditional physical assets or interests into digital form through digital technology. It involves the conversion of physical assets (e.g. real estate, stocks, bonds, etc.) or interests (e.g. intellectual property rights, ownership rights, etc.) into digital representations for storage, transmission, trading and management in a digital environment.

The purpose of asset digitization is to introduce traditional assets into the digital economy and to achieve programmability, divisibility, tradability and traceability of assets through the use of blockchain, cryptography, smart contracts and other technological means. This makes the trading of traditional assets more efficient, transparent and credible, and provides opportunities for wider market participation and capital flows.

Some applications of asset digitization include:

- Securitization: Physical assets (e.g., real estate, artwork) are transformed into digital securities through blockchain technology, making them tradable and liquid on a global scale;
- Creative Economy: Transforming intellectual property (e.g., music, movies, games) into digital assets through digital means, facilitating copyright protection, licensing and distribution;

- Cross-border Payments and Remittances: Utilizing digital assets and cryptocurrency technology to enable faster, lower-cost cross-border payments and remittances;
- Decentralized Finance (DeFi): decentralized financial services, such as lending, trading and derivatives transactions, by digitizing traditional financial assets (e.g., currencies, bonds, derivatives) and constructing financial protocols based on blockchain technology;
- Digital Identity and Ownership: Blockchain technology is utilized to establish and manage an individual's digital identity and ownership, enabling the individual to better control and manage their digital assets.

The digitization of assets had many potential benefits, including reducing transaction costs, improving liquidity, promoting market transparency and increasing the inclusiveness of capital markets. However, it also faces a number of challenges, such as imperfections in legal and regulatory frameworks, technological security and privacy issues. Therefore, a combination of technological, legal, regulatory and market factors need to be considered in promoting asset digitization.

AISec (Artificial Intelligence Security) can help us meet the security challenges of digital assets. Here are some of the ways:

- Anomaly Detection: AISec can be applied to digital asset monitoring and anomaly detection by analysing large amounts of data and transaction behaviour patterns to identify unusual activity or anomalous patterns. This can help in the early detection of potential security threats or attacks;
- Threat Intelligence: AISec can utilize machine learning and data mining techniques to analyse and process threat intelligence data from various security sources. This helps to understand the current threat environment in real time and take appropriate defense measures to protect digital assets;
- Intelligent Security Analytics: AISec can help analyse large amounts of security logs, event data and network traffic data to discover hidden attack patterns and vulnerabilities. By utilizing machine learning and deep learning algorithms, AISec is better able to identify and predict potential security threats;
- Automated Security Response: AISec can be integrated with an automated security response system to enable rapid response and countermeasures. When anomalous activity or security threats are detected, AISec can automatically trigger a response mechanism, such as blocking an attack, updating defense policies, or notifying the security team for further investigation and disposition.

It is important to note that while AISec has potential for digital asset security, it is not a panacea for all security problems. A secure and comprehensive solution should combine AISec with other security measures such as cryptography, access control, security auditing, etc. to provide comprehensive protection and risk management. In addition, human expertise and experience are still essential and can be combined with AISec to better protect digital assets.

5.3.1 CONTRACT SECURITY - A TOP SECURITY PRIORITY IN THE DIGITAL ASSET SPACE

With the rapid development of blockchain technology, smart contracts, as one of its representative applications, have been rapidly applied in various fields, such as finance and Internet of Things. However, due to the special structure and complexity of smart contracts, their security risk has gradually become an important issue, and the security vulnerabilities contained may lead to the contracts being exploited or tampered by attackers, thus jeopardizing the security of the whole blockchain system. In addition, the automatic execution characteristics and immutability of smart contracts make it extremely difficult to repair vulnerabilities and rollback operations. The development process of smart contracts involves multiple developers, which poses challenges for collaborative development and malicious code injection. At the same time, due to the complex logic and high testing cost of smart contracts, there exists a probability of security risks. Therefore, it is crucial to improve the security level of smart contracts and their ecosystems by adopting a series of effective measures. These measures include, but are not limited to, smart contract audits, secure programming models, code reviews, and ways to improve the development lifecycle of smart contracts. Only a combination of these means can provide a feasible and effective solution to the security problem of smart contracts.

It is for these problems and challenges in smart contract security that deep learning-based smart contract vulnerability detection has emerged in recent years. Compared with traditional rule-based detection methods, deep learning-based smart contract vulnerability detection can more accurately identify and categorize different types of vulnerabilities, and at the same time, it can also achieve high detection efficiency and fast response time. Therefore, this technology has a wide application prospect in the field of smart contracts and has become one of the hotspots for research in the field of smart contract security.

5.3.2 AISEC: VULNERABILITY DETECTION FOR SMART CONTRACTS AT SCALE

The goal of smart contract vulnerability detection is to discover code problems that may cause smart contracts to operate abnormally or that may be exploited by attackers, and to repair them as early as possible, so as to ensure the reliability, security and stability of the smart contract system. At the same time, such detection methods also aim to fulfil the expectation of business risk control, i.e., to effectively avoid potential risks and losses during the development, testing and launching of smart contracts.

Specifically, the objectives include, but are not limited to:

1) Discover and fix possible code vulnerabilities such as re-entry attacks, integer overflows, access control errors, etc.;
2) Minimize smart contract operation exceptions such as function rewrites, relocking, etc.;
3) Ensure the security and stability of the smart contract system to protect the user's assets;
4) Improve the accuracy of risk identification and minimize business losses.

Therefore, in deep learning-based smart contract vulnerability detection, comprehensive technical means as well as domain-adapted algorithmic models need to be adopted so that possible code problems can be discovered and solved as early as possible to provide a guarantee for the stable operation of smart contracts.

5.3.3 CURRENT RESEARCH AND PRACTICE OF SMART CONTRACT VULNERABILITY DETECTION

Currently, vulnerability detection for smart contracts can be mainly categorized into traditional methods and AI-based methods. Traditional methods include static analysis, dynamic analysis, and symbolic execution, which rely on the properties of the code itself and the execution path of the program to discover vulnerabilities. On the other hand, machine learning and deep learning-based methods build models with the support of a large number of well-labelled datasets, and identify whether there are vulnerabilities in the code of a new contract by learning the relationship between the data. Common machine learning algorithms include decision trees, support vector machines, etc., and commonly used deep learning algorithms include Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), and variants.

In the field of smart contract vulnerability detection, methods based on machine learning and deep learning have achieved some results. Some of the more advanced methods in engineering and academia include:

SmartCheck [20]: SmartCheck is a deep learning based static smart contract analysis method developed by Tikhomirov et al. It has achieved better results in performing blockchain smart contract detection. In the experiment, SmartCheck analyses a smart contract written in Solidity language and represents it as an XML-based intermediate representation, and detects it according to the XPath pattern to determine whether the smart contract has vulnerabilities. A comparison between SmartCheck and three manual detection methods is performed on a large dataset of real contracts, and the experimental results show that SmartCheck achieves significant improvements.

CBGRU [21]: CBGRU is a novel hybrid deep learning model for extracting feature vectors at different granularities by combining different word embeddings (Word2Vec, FastText) with different deep learning methods (LSTM, GRU, BiLSTM, CNN, BiGRU) and combining these feature vectors for smart contract Vulnerability Detection. The CBGRU hybrid model is demonstrated to have excellent performance in smart contract vulnerability detection through a series of experiments on the currently publicly available SmartBugs dataset-Wild. By comparison with previous studies, the CBGRU model has better detection performance.

MODNN [22]: The Multiple-Objective Detection Neural Network (MODNN) is a more scalable vulnerability detection tool for smart contracts that verifies 12 types of vulnerabilities, including 10 known threats. It employs implicit features and the Multiple-Objective Detection (MOD) algorithm to identify more unknown types of vulnerabilities, without requiring expert or predefined knowledge. It supports parallel detection of multiple vulnerabilities at the same time and is highly scalable, eliminating the need to train separate models for each vulnerability type, thus reducing

significant time and labour costs. And the authors of MODNN addressed the lack of smart contract vulnerability datasets by developing a Smart Contract Crawler (SCC) data processing tool. MODNN was evaluated using more than 18,000 smart contracts from Ethernet. Experiments demonstrated that MODNN achieved an average F1 score of 94.8% compared to several standard machine learning (ML) classification models.

MRNG [23]: Multi-Relational Nested Contract Graph (MRNG) is a novel multi-relational nested contract graph that aims to describe the rich syntactic and semantic information in smart contracts, as well as the relationships between data and instructions through edges and nodes. An MRNG expresses a smart contract, where each node represents a function in the smart contract, and each edge describes the invocation relationship of the function. In addition, its authors construct a Multi-Relational Function Graph (MRFG) for each function to represent the corresponding function. In addition, the authors propose a Multi-Relational Nested Graph Convolutional Network (MRN-GCN) for processing MRNGs, which extracts aggregated features of smart contracts by augmenting the graph convolutional layer of edges and the attention mechanism, and uses the feedforward network to locate vulnerable smart contract functions. This method can achieve better F1 performance.

SoliAudit [24]: SoliAudit is an approach to smart contract vulnerability assessment of Solidity bytecode using machine learning and fuzzing tests. Meanwhile, a gray-box fuzzy testing mechanism was created based on SoliAudit, including a fuzzy contract and a simulated blockchain environment to verify online transactions. Unlike other approaches based on machine learning and fuzzy testing, SoliAudit can perform vulnerability detection without expert knowledge or predefined vulnerability patterns. After evaluation, SoliAudit verified 18,000 smart contracts from Ethernet blockchain and CTF samples and detected 13 vulnerabilities with 90% Precision and can help identify reentrancy and overflow issues in smart contracts.

Some researchers have also utilized the Bidirectional Long Short-Term Memory Network (BiLSTM), which has been effective in the field of NLP, in conjunction with the Attention mechanism for identifying flaws in smart contracts [25]. The method treats the smart contract code as a sentence with context and evaluates 45,622 real smart contracts based on the BiLSTM-Attention model. The model is highly efficient to detect a large number of smart contracts quickly and obtains 95.4% Precision and 95.38% F1 performance.

With the above more advanced AISec-based smart contract vulnerability detection methods and tools at the current stage, we find that although there are many difficulties and challenges in the current smart contract vulnerability detection, it also opens up a new direction for exploring new technologies. In recent years, encouraging progress has been made by the engineering community and researchers in combining deep learning models to detect smart contract vulnerabilities, which also provides suggestions and directions for our future way forward.

5.3.4 THOUGHTWORKS METHODOLOGY AND PRACTICES

As a company actively exploring the field of digital assets, blockchain, and smart contracts, Thoughtworks has accumulated a certain amount of relevant experience and expertise. We always pay attention to the security of digital assets and the reliability of smart contracts, and try to contribute to the development and progress of these fields through continuous research and practice.

After research and exploration, we found that there are still the following directions that need to be researched for AISec-based smart contract vulnerability detection.

- Building a Unified and Standardized Smart Contract Vulnerability Dataset

If we want to make a breakthrough in deep learning-based smart contract vulnerability detection, we need a comprehensive smart contract vulnerability dataset. Currently, due to the lack of a standardized dataset, existing deep learning-based methods can only support the detection of a few contract vulnerabilities. Therefore, we need to build a unified and standardized dataset that covers as many vulnerabilities as possible to enable deep learning models to work better.

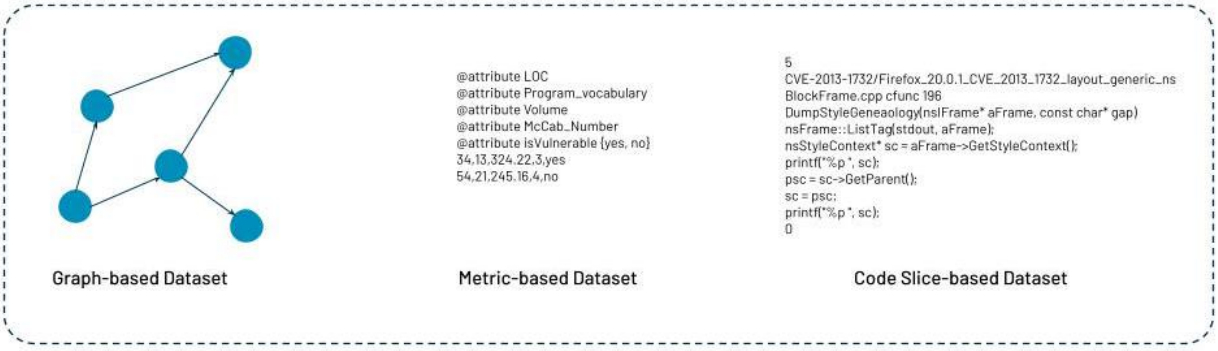

Figure: Source code-oriented multi-granular vulnerability datasets

- Training Reusable and Scalable Vulnerability Detection Models

With the explosive growth in the number of smart contracts, the corresponding security vulnerabilities become more and more complex and unpredictable. Currently, existing vulnerability detection methods based on deep learning mainly focus on model training for the vulnerabilities that have already been discovered. Therefore, whether they can quickly adapt to new types of vulnerabilities still requires further research. We believe that the rich security vulnerabilities in the open source smart contract ecosystem should be fully utilized to build reusable and extensible vulnerability detection models to cope with the emerging new smart contract vulnerabilities.

Smart contract itself has the data flow and control flow characteristics of the source code as well as the contextual semantic characteristics of the language itself, and these multi-dimensional static characteristics require appropriate representation and learning models for analysis and modelling. Considering that a series of mature algorithms have been developed in the fields of

image recognition and natural language processing, introducing these algorithms and adjusting them appropriately can also achieve good results in the field of smart contracts.

In multidimensional static feature processing, we can employ vector representation methods (e.g., word embedding) and tensor reconstruction to map features of different dimensions, such as code metrics, semantically related slices, and data flows, into the same vector space. This operation can provide an effective representation of multi-dimensional static features for subsequent deep learning algorithm analysis and vulnerability detection work. At the same time, this operation also needs to be considered to ensure the accuracy and interpretability of the feature characterization.

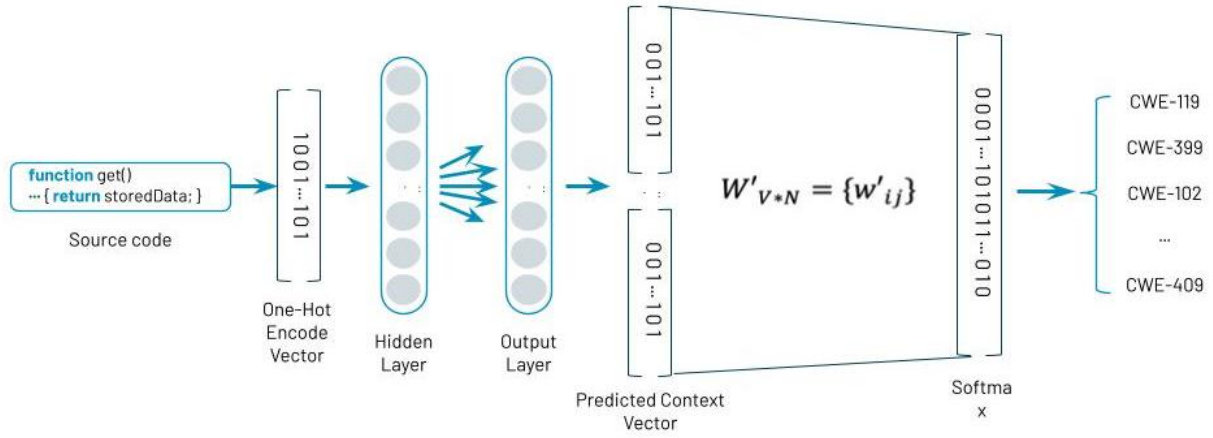

Figure: Encoder-Decoder Based Vulnerability Detection Models

Specifically, vector characterization can transform structured data such as code metrics and semantically related slices into high-dimensional vectors that can be compared and clustered in the same vector space. Similarly, tensor reconstruction techniques can transform multidimensional static features into shapes based on specific strategies to adapt them to the input requirements of different models. These processing tools provide the basis and support for the combination of multi-dimensional static feature processing and deep learning algorithms, so that detection models commonly used in other fields can be well generalized and applied to smart contracts.

- Integrated Modelling for Static and Dynamic Analysis

Static vulnerability detection can only characterize data based on static WYSIWYG features. However, for smart contract application scenarios that require automated execution, monitoring and enforcement of contract terms, dynamic monitoring and feedback mechanisms are equally critical. In the implementation process, smart contracts can be monitored, analysed and diagnosed in real time with the help of data flow analytics, so as to be able to dynamically intercept and deal with possible abnormal behaviours or improper operations during contract execution. This approach makes smart contracts more reliable and secure, and can effectively reduce potential risks and vulnerabilities. Therefore, in the application scenario of smart contracts, the dynamic monitoring and feedback mechanism is an indispensable and important part.

1) Vulnerability Detection Based on Generative Adversarial Model

Smart contract vulnerability detection method based on generative adversarial model is a technique that utilizes generative adversarial network (GAN) to achieve dynamic detection, which is capable of discovering, locating and repairing various security vulnerabilities and risks that may exist in smart contracts. The method utilizes the feature that generative models can generate representative code snippets to find covered vulnerabilities by generating corresponding code examples for specific vulnerability scenarios and testing these examples. At the same time, taint analysis techniques are used to identify potential data dependencies to further analyse and verify the security of smart contracts.

2) Automated Fuzz-based Vulnerability Detection

Fuzz testing can be used as part of the process of a smart contract vulnerability detection method based on generative adversarial modelling. According to the previous section, the usability and effectiveness of Fuzz testing has been verified by many researchers and Amber Group in other fields, and similarly smart contracts with explicit operational processes can also be used for vulnerability detection through Fuzz. Then, automated Fuzz is of high research value as it can liberate expert knowledge.

Specifically, the Fuzz test based on the Generative Adversarial Model generates different types of random input data, such as random numbers, random strings, random files, etc. These random input data are then fed into the smart contract, and the results and feedback are recorded. The Fuzz test repeats this process until a sufficient number of test cases have been completed or a specified number of vulnerabilities and defects have been found. By analysing the results and feedback generated by the tests, possible security vulnerabilities and anomalous behaviours of the smart contract can be identified. These problems can include integer overflows, null pointer references, logic errors, and so on. Once these issues are discovered through Fuzz testing, timely measures can be taken to fix the vulnerabilities and errors and improve the security and reliability of the smart contract.

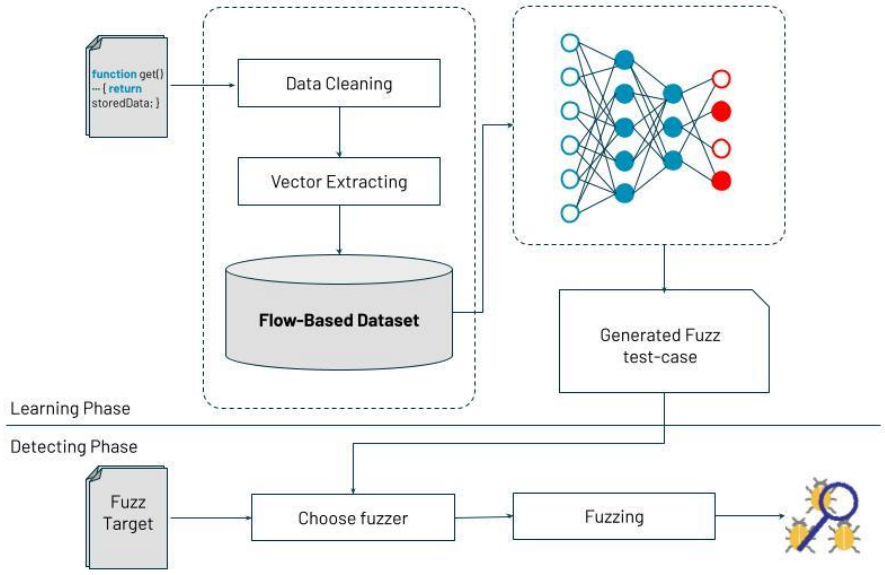

Figure: Generative and Fuzz-based Vulnerability Detection Models Overview

In addition to the above-mentioned approaches, we also noticed that many well-established methods are applied to this new field. Such as source code characterization based on multi-scale metrics, contextual semantic embedding that draws on natural language processing, grayscale graph characterization of source code, and generation-based symbol execution. In addition, transformer and attention methods, which have made a big splash in the field of natural language processing in recent years, have also been gradually introduced and applied in source code-oriented vulnerability detection. These methods have prompted Thoughtworks to continue to actively explore the combination of AISec with the digital asset and smart contract fields, as this is a very important and challenging field that requires continuous research and innovation to meet the needs of different business scenarios. We will actively embrace and utilize new technologies and tools to drive the industry forward and provide our clients with more efficient, accurate and reliable risk management services for digital assets, blockchain and smart contract business.

5.3.5 DIGITAL ASSET INDUSTRY OUTLOOK FOR AISEC ADOPTION

We believe that applying security detection and analysis tools based on artificial intelligence and deep learning to business risk control of digital assets, blockchain and smart contracts is a crucial strategic direction. Through scalability and rapid feedback, we expect to achieve accurate identification and management of business risks. However, we are also well aware that there are a number of challenges that need to be overcome in order to automate, improve accuracy and reduce false positives and omissions, with the lack of mature algorithms being one of the issues that must be addressed today. In addition, finding the right characterization method is also a key challenge.

Despite the many difficulties we face, we believe that through continuous research and exploration we will gradually overcome these challenges and provide high-quality services to our clients. Thoughtworks looks forward to driving the development of AI technology in the field of digital asset, blockchain and smart contract business risk management, and endeavours to innovate and improve the existing technological solutions in order to meet the new challenges that keep emerging. We look forward to working hand-in-hand with our clients and partners to realize our vision.

VI. GLOSSARY

Fuzzy test

Fuzzy testing (aka. fuzz testing or fuzzing) is a software testing technique. The core idea is to feed automatically or semi-automatically generated random data into a program and monitor for program exceptions, such as crashes, assertion failures, to detect possible program errors, such as memory leaks. Fuzzy testing is often used to detect security vulnerabilities in software or computer systems.

HSM

Hardware Security Modules (HSMs) are specialized cryptographic processors designed to protect the lifecycle of cryptographic keys. By securely managing, processing and storing cryptographic keys in a reliable and tamper-resistant device, the Hardware Security Module has become the trusted starting point for protecting cryptographic infrastructures for the world's most security-conscious organizations.

MDR

Managed Detection and Response (MDR) Service Managed Detection and Response, is a service that can provide customers with remotely delivered Modern Security Operations Center (Modern SOC) functionality.

Enterprise organizations can leverage these capabilities for 1) rapid detection, 2) analysis, 3) investigation, 4) proactive mitigation, and 5) containment of threats. MDR service providers offer a one-stop shop experience.

MDR (Managed Detection & Response) service vendors provide threat content and threat analytics based on relevant data from hosts, networks, applications, and the cloud, using means that include threat intelligence and manual and automated incident response, such as incident classification, investigation, quarantine, and other actions. Threat hunting capability is an advanced capability that expands real-time threat detection capabilities and enables the discovery of attack-related technologies especially for those attacks that can bypass traditional security defences and detection means.

Privacy by Design

Privacy by Design refers to a systems engineering approach originally developed by Ann Cavoukian and formalized in a joint report on privacy-enhancing technologies by a joint team of the Information and Privacy Commissioner of Ontario (Canada), the Netherlands Data Protection Authority and the Netherlands. 1995 Applied Science Research Organization. The Privacy by Design framework was released in 2009 and adopted by the International Conference of Privacy Commissioners and Data Protection Authorities in 2010. Privacy by Design requires that privacy be considered throughout the systems engineering process. The concept is an example of value-sensitive design, where human values are considered in an explicit manner throughout the process. Privacy by Design consists of seven privacy principles:

1) Proactive not Reactive; Preventative not Remedial;
2) Privacy as the Default Setting;
3) Privacy Embedded into Design;
4) Full Functionality – Positive-Sum, not Zero-Sum;
5) End-to-End Security – Full Lifecycle Protection;
6) Visibility and Transparency – Keep it Open;
7) Respect for User Privacy – Keep it User-Centric

Red Teaming

Red Teaming was originally a military concept, referring to the army's military exercises, in which the red side is usually the defending side and the blue side is the attacking side. In the field of information security, it refers to network security attack and defense drills, the blue army simulates real attacks to assess the security of the existing defense system; the red side can find out more about their own security problems through the drill, and quickly complete the checking and mending.

Secure Multi-Party Computing (MPC)

Secure Multi-Party Computing (MPC) is a cryptographic tool that allows multiple parties to perform computations using their combined data without having to reveal their personal inputs. Invented by Chinese computer scientist Yao Qizhi, MPC distributes computations between multiple parties by using complex encryption. In the context of digital assets, MPC can be used as an alternative to individual private keys for signing transactions. MPC distributes the signing process among multiple computers. Each computer has a private piece of data representing a share of the key, and they work together to sign transactions in a distributed manner.

Smart Contract Audit

Smart contract auditing involves a detailed analysis of a protocol's smart contract code to identify security vulnerabilities, poor coding implementations, and inefficient code before proposing solutions to address these issues. Auditing helps ensure the security, reliability and performance of decentralized applications across Web3.

SOAR

Security Orchestration, Automation and Response (SOAR) is a set of capabilities used to protect IT systems from threats.

SOAR refers to three major software functions used by security teams: case and workflow management, task automation, and centralized management of accessing, querying, and sharing threat intelligence. the term SOAR comes from the analyst firm Gartner. IDC refers to the concept as "Security Analysis, Intelligence, Response, and Orchestration" (AIRO), while Forrester uses the term Security Automation and Orchestration (SAO) to describe the same function. IDC refers to the concept as "security analysis, intelligence, response and orchestration" (AIRO), while Forrester uses the term "security automation and orchestration" (SAO) to describe the same function.

SOAR is typically implemented in coordination with an organization's Security Operations Center (SOC). The SOAR platform monitors threat intelligence feeds and triggers automated responses to security issues, which helps IT teams quickly and effectively mitigate threats across many complex systems.

UEBA

User and Entity Behaviour Analytics (UEBA) is a user and entity behaviour analysis technology, UEBA is more concerned about the abnormal behaviour of people, the main body of the behaviour is usually the internal staff of the enterprise. UEBA technology based on massive data on the internal user's abnormal behaviour or internal threat prediction, direct "people" perspective gives the decision to catch the "bad guys", take the initiative to stop before the data leakage and provide a reliable basis for security analysts. UEBA technology predicts the abnormal behaviour of internal users or internal threats based on massive data, and gives judgment directly from the perspective of "people", catches the "bad guys", takes the initiative, stops data leakage before it occurs, and provides a reliable basis for security analysts.

VII. REFERENCE

[1] "The HamsterWheel: an In-Depth Exploration of a Novel Attack Vector on the Sui Blockchain", Certik , June 19, 2023

[2] "Fuzzing the Native NTFS Read-Write Driver (NTFS3) in the Linux Kernel", Black Hat Asia 2023 , May 12, 2023

[3] "Fuzzing the Latest NTFS in Linux with Papora: An Empirical Study" Amber Group May 2023

[4] "Position Exchange's Re-Entrancy Loophole Explained," Amber Group May 9, 2022

[5] CVE-2022-48423, Amber Group, March 18, 2023

[6] CVE-2022-48424, Amber Group, March 18, 2023

[7] CVE-2022-48425, Amber Group, March 18, 2023

[8] "Dinosaur Eggs' LiquidityPool Loophole Explained", Amber Group , November 16, 2021

[9] "Strips Finance's Price Manipulation Vulnerability Explained", Amber Group , July 29, 2022

[10] "Mai Finance's Oracle Manipulation Vulnerability Explained", Amber Group, December 20, 2022

[11] "https://github.com/ambergroup-labs/papora", Amber Group, April 2023

[12] "Web3 Project Security Practice Requirements v0.1", Slow Fog, April 6, 2023

[13] "Exploiting the Profanity Flaw", Amber Group, September 30, 2022

[14] "Ethereum is a Dark Forest", Dan Robinson, August 29, 2022

[15] "Rescuing Schrodinger's Cat in DeFi Dark Forest" Victor Fang, AnChain.AI, October 2020

[16] "The $4 Billion Digital Asset Hacking Problem May Finally Have a Solution: Web3SOC", AnChain.AI, March 21, 2023

[17] "An Analysis of the Globalized Regulation of Cryptocurrency Exchanges - Insights from the Collapse of FTX, the World's Third Largest Cryptocurrency Exchange", Jintiancheng, January 17, 2023

[18] "Privacy By Design Theoretical Architecture and Technical Practice", Cloud Security Alliance Greater China (CSA-GCR), February 4, 2023

[19] "Exploring Product Scenarios for Privacy by Design", Big Data Technology Standards Promotion Committee, June 5, 2023

[20] Tikhomirov, S., Voskresenskaya, E., Ivanitskiy, I., Takhaviev, R., Marchenko, E. and Alexandrov, Y., 2018, May. smartcheck: static analysis of Ethereum smart contracts. in Proceedings of the 1st international workshop on emerging trends in software engineering for blockchain (pp. 9-16).

[21] Zhang, L., Chen, W., Wang, W., Jin, Z., Zhao, C., Cai, Z. and Chen, H., 2022. cbgru: A detection method of smart contract vulnerability based on a hybrid model. Sensors, 22(9), p.3577.

[22] Zhang, L., Wang, J., Wang, W., Jin, Z., Su, Y. and Chen, H., 2022. smart contract vulnerability detection combined with multi-objective detection. Computer Networks, 217, p.109289.

[23] Liu, H., Fan, Y., Feng, L. and Wei, Z., 2023. Vulnerable Smart Contract Function Locating Based on Multi-Relational Nested Graph Convolutional Network. Journal of Systems and Software, p.111775.

[24] Liao, J.W., Tsai, T.T., He, C.K. and Tien, C.W., 2019, October. soliaudit: Smart contract vulnerability assessment based on machine learning and fuzz testing. fuzz testing. in 2019 Sixth International Conference on Internet of Things: Systems, Management and Security (IOTSMS)(pp. 458-465). IEEE.

[25] Qian, C., Hu, T. and Li, B., 2022, December. A BiLSTM-Attention Model for Detecting Smart Contract Defects More Accurately. in 2022 IEEE 22nd International Conference on Software Quality, Reliability and Security (QRS)(pp. 53-62). IEEE.

[26] ISACA. (2021, August 26). ISACA Blockchain Framework Audit Program. ISACA.

ANNEX. AMBER INDUSTRY ENABLING PROGRAM FOR CYBERSECURITY PRACTICES FOR DIGITAL ASSETS

Amber Group, a leading provider of crypto asset management and trading services, is committed to delivering its superior security capabilities, professional security consulting, and advanced security products to a broader user base through external empowerment.

Currently, Amber Group offers a comprehensive crypto-financial security and compliance solution that leverages AI and Web3 Threat Intelligence. This all-in-one solution provides clients with a closed-loop security system, empowering them with a financial-grade security capability. By utilizing combinable and worry-free security hosting solutions, clients can swiftly acquire the necessary virtual asset operation qualifications and stay informed about security compliance regulatory requirements. This positions clients to seize early business opportunities in the emerging financial landscape.

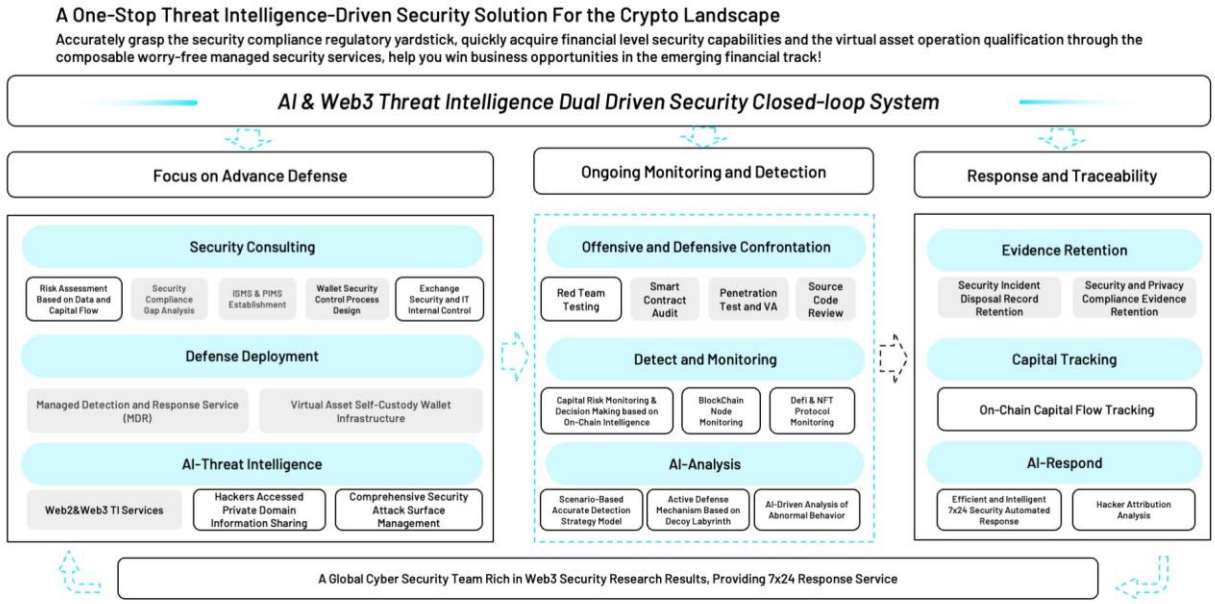

Figure: One-Stop Crypto Financial Security & Compliance Solution

Amber Group has established a reputation for excellence in the field of security through its tight security architecture and efficient risk management practices. The company employs advanced encryption technologies, multiple authentication and comprehensive security auditing measures to ensure that users' assets and transaction information are always in the most secure state. The accumulation of these security capabilities has made Amber Group one of the first choices trusted by many users and partners.

As a professional security consulting provider, Amber Group draws on its deep industry experience and dedicated team of professionals to provide organizations and individuals with comprehensive guidance on the security of crypto assets. By assessing and identifying potential security risks, Amber Group tailors' solutions to help clients establish robust security strategies and processes.

In their collaboration with clients, Amber Group not only imparts security best practices but also delivers comprehensive security training. This initiative aims to support clients in effectively addressing the diverse security challenges they encounter in their daily operations.

These specialized security consulting services not only provide clients with practical solutions, but also enhance the security awareness and capability of the entire industry.

In addition to security consulting, Amber Group specializes in developing and delivering security products and solutions to meet the security needs of a wide range of users. The company continues to develop and improve various security technologies and products, including digital asset security and privacy compliance consulting services, Managed Security Detection Response (MDR) services, self-hosted wallet infrastructure for virtual assets, security defense deployment services, hacker-touch private domain intelligence sharing services, and on-chain transaction monitoring and auditing tools. With their advanced features and high reliability, these security products help users better protect and manage their crypto assets. By exporting security products to the outside world, Amber Group not only provides users with practical tools, but also promotes security standards and technological advances in the entire crypto asset management industry.

To summarize, Amber Group delivers its outstanding security capabilities, professional security consulting and advanced security products to a wider user community through external empowerment. The company maintains a humble and objective attitude, backed by its outstanding security reputation and technical strength, to provide users with comprehensive security protection. Whether through the sharing of security capabilities, the provision of security consulting, or the development and output of security products, Amber Group is constantly committed to promoting security standards and technological innovation in the cryptographic field, creating a more secure and reliable environment for the development of the industry and the trust of users.

1 OPERATIONAL SECURITY RISK ASSESSMENT AND RISK MANAGEMENT SERVICES BASED ON DATA AND FINANCIAL FLOWS

In the field of digital assets, data is regarded as oil and gold, and is used as a source of core competitiveness for enterprises. There is a very close relationship between data and fund in this field, and once sensitive data such as private keys, auxiliary words and credentials are lost, it will bring about actual financial losses. Therefore, comprehensive identification, analysis, and evaluation of the data flow and fund flow of digital asset management organizations is an effective method of security risk management in the field of digital assets, which can quickly help digital asset management organizations to quickly find high-risk issues that may lead to the loss of the company's funds and provide corresponding solutions.

Over the years of security and compliance operations, Amber Group has formed a "business security risk management methodology based on data and fund flows" and accumulated mature experience in clue mining, threat modelling, assessment and analysis in various risk control

domains, which enables us to quickly find out where the digital asset security risks are by means of research and interviews, document inspection, system and walk-through testing. We are able to quickly find out where the security risks of digital assets lie through research and interviews, document inspection, and system walk-through testing. After identifying the relevant risks based on the business security risk assessment methodology of data and fund flow, we can build an information security and privacy management system (ISMS & PIMS) for our clients that meets the regulatory compliance requirements, so as to equip our clients with comprehensive information security management policies, processes and norms.

The methodology of this risk management and its value are briefly described below:

1.1 DATA FLOW RISK ASSESSMENT

The methodology of data flow risk assessment, the research results incubated by data security and privacy protection governance practices, and the assessment service formed by combining the data flow characteristics of the digital asset field. Data flow risk assessment focuses on confidential and sensitive data situations such as password, credential, access key, secret key, private key, mnemonic, transaction algorithms, core code, data models and customers' personal privacy data. On the one hand, the assessment is made from the perspective of data life cycle, around the stages of data collection, transmission, storage, use, exchange, sharing, and destruction; on the other hand, the assessment is made from the aspects of technical architecture, such as system architecture, network architecture, cloud architecture, data architecture and so on, covering the environment of the cloud, data centres, and workplace office networks. Sort out the connection between internal systems and the data interaction with external suppliers. Finally, a data flow diagram will be delivered, which can be used as a base input for threat modelling.

1.2 RISK ASSESSMENT OF FUND FLOWS

Fund flow risk assessment methodology, which is based on the capabilities extended from the digital asset business risk control framework. The fund flow risk assessment methodology is derived from the digital asset business risk control framework and focuses on evaluating risks associated with fund flows. It encompasses two main categories: CeFi (Centralized Finance) and DeFi (Decentralized Finance) digital asset businesses. This methodology enables a comprehensive assessment of potential risks in both types of operations.

1) **CeFi:** CeFi is a fund flow interaction model between digital asset management platforms and traditional centralized exchanges and third-party asset custodians. The flow of fund is mainly manifested in the following business scenarios:
   - Transfer of digital currency between self-hosted wallets of digital asset management platforms and self-hosted wallets of centralized exchanges (CEX);
   - Digital Asset Management Platform self-hosted wallets and third-party hosted wallets for digital currency transfers;

- Third-party hosted wallets for internal trading desks, digital currency transfers between sub-accounts;
- Digital Asset Management platform with client self-hosted wallets for top-ups and withdrawals.

Service Value Summary: CeFi's fund flow security control focuses on evaluating internal control measures such as account management, authority management, API management, and approval of all types of asset transfers, operation traces, and after-the-fact reviews for centralized exchanges (CEX) and third-party hosted wallets, providing customers with protection against account abuse, loss of control of APIs, loss of funds, internal collusion, misappropriation of funds, inconsistency of financial reconciliation and complicity in key business processes.

2) Defi: Defi is a fund flow interaction model between digital asset management platforms and decentralized exchanges (DEX), Web3 project-side smart contracts, and wallets of third-party asset custodians. The flow of funds is mainly manifested in the following business scenarios:
   - The digital asset management platform self-hosts asset transfers between wallets and smart contract addresses on decentralized exchanges (DEX);
   - The digital asset management platform self-hosts the transfer of assets between the wallet and the smart contract address of the Web3 project side;
   - Asset transfer between a third-party asset custodian wallet and a smart contract address on a decentralized exchange (DEX);
   - Asset transfer between the wallet of the third-party asset custodian and the smart contract address of the Web3 project side.

Service Value Summary: DeFi's fund flow security control focuses on evaluating the digital asset management platform's DeFi project wallet creation and authorization process, third-party asset custodian's wallet creation and authorization, smart contract creation and deployment process, smart contract auditing, code review, transaction process testing, wallet withdrawal address whitelisting process, authentication of transaction accounts and APIs, and real-time wallet address asset monitoring and alerts. It can greatly ensure the manageability, control, availability and visualization of customers' transactions in DeFi.

2 WEB3 AND DIGITAL ASSET SECURITY COMPLIANCE CONSULTING SERVICES

Amber Group has completed the exploration and practice of compliance requirements in most major economies around the world on the path of Web3 and digital asset security compliance operation, which includes Singapore, Hong Kong, China, the United States, Canada, the European Union, Japan, South Korea, Australia, the Middle East and other countries and regions. By summarizing and precipitating the practice, effective Web3 and digital asset security compliance consulting services have been formed, which can provide the industry with security compliance consulting services to satisfy the regulators around the world.

Digital asset managers facing the intricacies of global regulatory compliance requirements should build a solid foundation of security compliance before tailoring appropriately to suit the differences in jurisdictions to accommodate local regulatory requirements.

TYPICAL CASE PRESENTATION: HONG KONG VIRTUAL ASSET SERVICE PROVIDER (VASP) COMPLIANCE REQUIREMENTS

Take Hong Kong as an example, its "Guidelines for Virtual Asset Trading Platforms Operators" on Virtual Asset Service Providers (VASPs) have clear chapters on cybersecurity requirements, while a number of security requirements are scattered in other chapters, including requirements on vendor due diligence, Token Admission, and asset custodianship, etc. If there is a lack of professional analysis of security compliance gaps, it will be impossible to implement the relevant cybersecurity requirements against the standard requirements in a comprehensive manner.

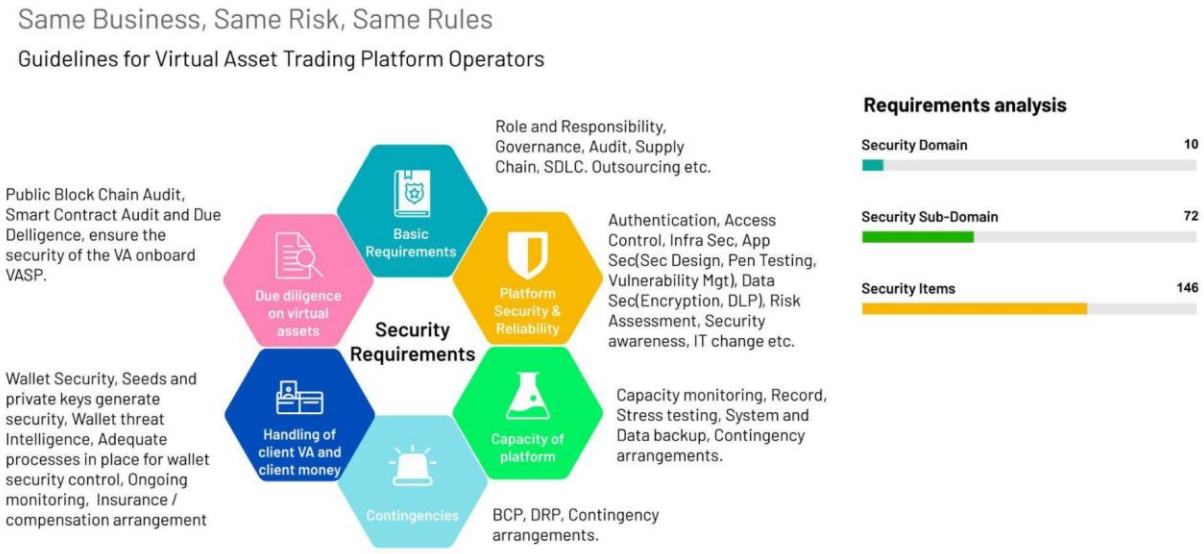

Figure: Hong Kong VASP Security Requirements

According to Amber Group's analysis of Hong Kong VASP security requirements, as shown in the figure, a total of 10 Security Domains, 72 Security Sub-Domains and 146 Security Requirements have been sorted out, which mainly cover the following aspects:

- Basic Requirements: including cybersecurity principles, governance, resource assurance, roles and responsibilities, audit requirements, R&D security lifecycle, outsourcing risk management, and more;
- Platform Security & Reliability: including authentication, access control, infrastructure security (firewall, WAF, IPS & IDS, EDR, SIEM and SOC), penetration testing, source code security review, vulnerability management, data security (encryption, DLP), risk assessment, security awareness, IT changes, etc.;
- Capacity of Platform: including capacity monitoring, logging, stress testing, system and data backup and recovery, contingency planning, etc.;

- **Contingency measures:** including BCPs, DRPs, contingency plans and emergency drills, etc.;
- **Handling of client VA and client money:** including wallet security, seed and private key generation security, wallet threat intelligence, adequate wallet security controls, continuous monitoring, insurance and claims arrangements, and more;
- **Due Diligence on Virtual Assets:** including public chain auditing, smart contract auditing and due diligence, security of token management, and so on.

After analysing the digital asset security compliance requirements in each jurisdiction, it is possible to identify the gap between the current state of security and the compliance requirements, and propose to the digital asset management organization the security rectification recommendations and overall compliance solutions with the best input-output ratio.

Service Value Summary:

Amber Group's Web3 and digital asset security compliance consulting services use gap analysis and risk assessment as the entry point, information security and privacy management system construction as the base, and Web3 & digital asset scenarios to form a holistic security compliance solution that meets the regulatory compliance requirements, which can assist companies interested in obtaining digital asset compliance licenses to become cybersecurity ready quickly. It can help enterprises interested in obtaining digital asset compliance licenses to quickly become ready in terms of network security.

3 PRIVACY TECHNOLOGY AND COMPLIANCE SERVICES BASED ON PRIVACY BY DESIGN

Amber Group's Privacy Engineering Practice is a comprehensive governance framework that integrates data security and privacy protection. Its main objective is to embed Privacy by Design & Default into the DevSecOps product development process. This ensures that privacy elements are considered early in the product development process, creating a "left shift in security and privacy" goal that can prevent data misuse, data leakage, and privacy compliance risks within the organization.

After years of industry insights and on-the-ground practice, a mature one-stop privacy technology platform has been developed, which fully realizes the Privacy by Design concept. This platform can provide the industry with one-stop privacy compliance solutions based on privacy technology and help digital asset management organizations enhance digital trust.

- Provide enterprise privacy protection governance consulting services to establish a framework that meets the requirements of data privacy compliance (e.g., GDPR, CCPA, PDPA) in various jurisdictions around the world;
- Establish a sound privacy design specification for your organization based on Privacy by Design and privacy engineering methodologies;
- With a cutting-edge privacy program management platform, we solve privacy compliance management issues for organizations such as data asset management, data mapping,

consent management, privacy notice management, data subject rights, privacy impact assessment and privacy incident management.

Service Value Summary:

In the Web3 era, having a 100% anonymized privacy experience was the ideal for crypto-native residents. However, as data compliance regulation, digital asset compliance regulation, and industry self-regulation rules become stricter worldwide, users may have to submit their personal data to digital asset management institution for compliance verification. This will lead to the centralization of managing personal contact data, KYC biometrics data, and personal financial transactions, which could trigger an even bigger digital trust crisis if customer data privacy is compromised.

To address this issue, privacy technology based on Privacy by Design (PbD) and compliance services can provide clients with a holistic privacy protection solution that meets compliance requirements. By using cutting-edge privacy management platforms and privacy policies from the perspective of enterprise privacy governance, this solution enhances trust in the digital age and gives privacy rights back to users.

4 DIGITAL ASSET CUSTODY WALLET SOLUTION

The development of digital asset custody solutions has gone through several key phases. Initially, due to the emergence of cryptocurrencies, individual users started using their own wallets for asset management. As interest in digital assets increased among institutions and corporations, third-party custody services rose to prominence, providing users and organizations with more specialized security and reliability. Amber Group adopted industry-leading digital asset custody solutions and introduced more advanced technology and security measures to build comprehensive solutions that meet regulatory requirements for functionality, compliance, and security through hot and cold wallet technologies such as multi-signature wallets, multi-party computing (MPC), and HSM. This ensures that their digital asset custody solutions meet the highest security standards.

4.1 ONE-STOP DIGITAL ASSET CUSTODY SERVICES

Amber Group has a regulated and insured custodial entity with a multi-wallet infrastructure that provides a one-stop digital asset custody service for individual and institutional clients. The escrow service has the following features:

1) Regulated Compliance Custody
   Amber Group is licensed as a Trust or Company Service Provider in Hong Kong.
2) Multi-wallet Infrastructure with Institutional-grade Security
   Hot wallet and 100% offline cold wallet infrastructure with institutional-grade security in wallet design, deployment and control.

4.2 MULTI-WALLET INFRASTRUCTURE

Amber Group has developed a multi-wallet infrastructure comprising MPC hot wallets, proprietary HSM-based warm wallets, and completely offline cold wallets, ensuring compliance with regulatory standards and facilitating seamless asset transfers, thereby offering clients a comprehensive solution for asset custody.

4.3 AMBER GROUP HSM TOTAL SOLUTION

Amber Group's HSM overall solution is an integrated solution based on asset custody regulatory requirements in various regions, combined with industry-leading technology standards and internal control processes. The solution has the following features:

- Meets industry-leading FIPS 140-3 security standards;
- Support life cycle security management of digital asset private key, including private key generation, storage and operation, backup and recovery;
- Enterprise digital asset transfer has a perfect wind control process and multi-level approval mechanism;
- Hot and cold wallet separation and a well-established wallet infrastructure can provide organizations with the ability to manage both cold storage and hot wallet assets;
- It can be docked to the enterprise business system through the integrated API to provide the enterprise business system with functions such as digital asset deposit and withdrawal;
- It also meets the regulatory asset custody requirements of Hong Kong VASP and Japan CAESP.

When deployed as a cold wallet approach, it consists of two main parts: online and offline operations.

- The offline part: Digital asset custody server and Airgapped Vault software module. The Airgapped Vault software module is installed on a dedicated computer which is physically isolated along with the custody server in a safe house
- The online part: Airgapped Wallet service connects to blockchain networks. Management, configuration and transaction operations are initiated via the wallet management system and wallet business system. Operators use a dedicated biometric authentication USB drive to transfer information to be signed or signed information, ensuring the custody server never goes online.

4.4 TECHNOLOGY ADOPTION FOR MPC (SECURE MULTI-PARTY COMPUTATION)

Ensuring the secure storage and transfer of cryptocurrencies is critical for expanding business operations, and Amber Group's related businesses are further enhanced by the multi-party computation (MPC) technology infrastructure. Amber Group utilizes MPC technology solutions for high-speed transactions and also ensures security. The MPC technology solutions adopted by Amber Group provide infrastructure for the secure transfer, storage, and issuance of digital assets. Through MPC technology and chip-level hardware isolation techniques, the security of digital assets can be effectively protected. This innovative approach safeguards customers' private keys, protecting API keys and deposit addresses from network attacks and internal fraud. Meanwhile, key management services based on MPC eliminate single points of failure. With the secure transfer environment enabled by the solution, Amber Group can protect the mobilization of customers' digital assets across exchanges, custodians, OTC brokers, hot wallets, and cold storage. Additionally, the solution provides end-to-end insurance for assets stored and in transit as a risk mitigation measure.

4.5 SUMMARY OF THE VALUE OF DIGITAL ASSET CUSTODY SERVICES

Amber Group's digital asset custody solutions have diverse capabilities, with custodial services currently able to effectively support global customers across different countries, asset types, and needs. Based on assessments of market trends and regulatory compliance insights, self-custody and third-party custody solutions will likely coexist in the future, and even the same company may use both solutions concurrently.

Amber Group employs a multi-wallet infrastructure that can be adapted based on different business requirements to ensure the highest security standards for digital asset custody. By utilizing MPC technology, some assets can flow more rapidly. By using HSM technology, it can comply with the regulatory asset custody requirements like Hong Kong VASP and Japan CAESP. The combination of both solutions will provide customers greater flexibility for digital asset custody.

5 WEB3 MDR SECURITY DETECTION AND RESPONSE HOSTED SOLUTION

MDR (Managed Detection and Response) is an emerging concept of cybersecurity services, referring to security detection and response services to be hosted by a professional third-party security organization, through the integration of the traditional security operations center (SOC) and security information and event management (SIEM), and the use of AI and machine learning and other technologies to improve customer's ability to By integrating the traditional security operation center (SOC) and security information and event management (SIEM), and using technologies such as AI and machine learning to improve the customer's ability to detect and respond to network threats, it greatly reduces the cost of users to set up their own professional security attack and defense teams and build security protection facilities.

The development of MDR can be traced back to the emergence of SOC. In the field of Web3 and digital assets, digital assets are closely associated with huge sums of money, which also attracts more hacker organizations to frantically attack and loot, the traditional security operation center (SOC) can no longer meet the needs of this field, and enterprises need to superimpose the chain security capabilities of Web3 on the traditional security foundation in order to effectively respond to security threats.

The Web3 SOC developed by AnChain.AI is based on the traditional SOC and overlaid with the Web3 on-chain listening and data analysis capabilities according to the IPDRR (Identification, Defense, Detection, Response, Recovery) methodology of the NIST CyberSecurity Framework, which provides users with more accurate Web3 threat intelligence and feeds the intelligence into the whole process of prior key defense, detection and response, and recovery and traceability in a timely manner by automated means, making the traditional SOC add the Web3 eye in the sky, which can be utilized in a shorter time and with higher efficiency. It provides users with more accurate Web3 threat intelligence, and through automation, timely feedback of intelligence into the whole process of ex-ante focused defense, ex-ante detection and response, and ex-post recovery and traceability, so that the traditional SOC has added Web3 eyes in the sky, and is able to respond to and recover from security incidents in a shorter time and with higher efficiency, and comprehensively reduces the security risks in both the traditional Web2 domain and the emerging Web3 domain. The product has been highly recognized by the industry as it won the Innovation Sandbox Award at RSA 2023, an international cybersecurity event.

Amber Group's Web3 MDR is based on traditional security capabilities, combined with the on-chain security analysis capabilities provided by AnChain.AI's Web3 SOC, EVM transaction simulation capabilities, and machine-learning-based smart contract anomaly detection capabilities, to form a hosted service that has the ability to defend, detect and respond to threats to Web3 and digital assets.

The functions of Web3 MDR mainly include: real-time monitoring, anomaly detection, intrusion analysis, and threat intelligence analysis of traditional network security and Web3 chain security. Among them, real-time monitoring is the most critical function, which can monitor various behaviours occurring in the enterprise network and on the chain in real time, and detect and deal

with abnormal events in a timely manner. In addition, in terms of threat intelligence analysis, Web3 MDR can utilize big data technology and AI algorithms to collect threat intelligence and all kinds of monitoring and auditing data from the global scope, and analyse its impact on the enterprise, so that the enterprise can carry out corresponding risk prevention work.

Amber Group has built an MDR platform based on the digital asset industry and the experience gained from fighting against hacktivist organizations, with the core of the MDR platform covering four main areas:

- Terminal Compliance and Attack Detection: By installing and deploying Agents in protected terminals to realize multi-faceted monitoring of terminals, it realizes real-time detection and discovery of terminal compliance and security items and potential attack behaviours and malicious files;
- Log aggregation and centralized analysis platform: Aggregation accepts data from all Agents and multi-channel collection, and according to the configuration and rules and policies for comprehensive analysis and detection, which occurs on the potential risk of attack alarms;
- Web3 and on-chain security detection: Monitoring and detection systems are used to identify on-chain cybersecurity events in a timely manner, enabling early detection and effective response. For example, machine learning is used to detect fraudulent actors on the Elrond blockchain and apply preventive countermeasures (e.g., blocking transactions) to achieve control.
- Managed Incident Response: By identifying the enterprise's assets, systems, data and other resource information beforehand, an effective incident response plan is established, so that the efficiency of response during the incident is greatly improved. Medium- and high-risk events in the response process will be distributed to the corresponding event hosting service team through the event distribution mechanism, and the relevant team relies on SOAR & AI to realize rapid and accurate analysis and response to medium- and high-risk events.

5.1 TERMINAL COMPLIANCE AND ATTACK DETECTION

Terminal compliance check is an indispensable part of enterprise information security management. With the development of enterprise information technology, the number and types of terminal devices are increasing, and the means of network attacks are also becoming more and more complicated, which brings great challenges to enterprise information security. Terminal compliance checking can discover the possible vulnerabilities and security risks on terminal devices in a timely manner, and minimize the losses caused by information leakage or hacker attacks.

Amber Group's endpoint-based protection software and the joint integration of three-party software and audit logs realize a series of capabilities for endpoints, including asset inventory, asset vulnerability discovery, and standards-based compliance checking, etc., to ensure that endpoints accessing the office production network can always stay on the top of the security and compliance line, and support regulatory requirements, including PCI DSS, GDPR, HIPAA, NIST 800-500, TSC, and so on. HIPAA, NIST 800-53, TSC, and more.

Terminal attack detection is one of the important means to guarantee computer security, and we have established a perfect terminal attack detection mechanism based on MITRE's ATT&CK concept. In the current rhythm of attack and defense confrontation, terminal equipment is often the target of attackers, so it is necessary to take the necessary measures to prevent and detect attacks from the terminal, and because of the great operability of the terminal environment, on which the means of protection can be based on the detection and discovery of attacks, but also bring other more potential possibilities:

1. Preventing Data Leakage: An endpoint attack can result in the leakage of sensitive information that can seriously affect an individual or organization;
2. Reduced Business Downtime: If an endpoint is attacked, it may cause the system to crash or run slowly, resulting in business downtime;
3. Determine the Source of the Attack: Terminal attack detection allows you to determine whether the attack is from external or internal sources, which helps to further strengthen security protection.

Amber Group's endpoint-based protection software employs log monitoring, virus detection, behavioural analysis, anomaly detection, and AI diagnostics to achieve multi-dimensional and integrated security attack risk detection of endpoint behaviour.

5.2 LOG AGGREGATION AND CENTRALIZED ANALYTICS PLATFORMS

In the overall architecture of the MDR platform, the analytics platform located in the center of the whole is the core basic component of the MDR solution, which undertakes the following functions for the entire security protection system:

1) Gather Comprehensive Threat Intelligence: The platform can gather threat intelligence from multiple sources, including hacking, vulnerabilities, espionage, and other types of threats;
2) Real-time Monitoring and Detection: The platform enables real-time monitoring and timely detection of various abnormal activities and threatening behaviours such as DDoS attacks, malware and data leakage;
3) Multi-Dimensional Automated Analysis: The platform can perform multi-dimensional analysis of data through automated analytics to discover threat behaviours hidden behind massive amounts of data;
4) Rapid Response and Response: The platform automates response and defense, including intrusion detection, tracing, blocking, quarantine, and other means, enabling organizations to respond quickly to threat events and reduce loss and risk.

Amber Group's MDR analytics platform, backed by years of experience in the industry, balances power and efficiency to provide users with the following platform capabilities:

1) Log Aggregation: The platform supports access to almost any text-based log data, and allows the collection and aggregation of log data to the platform through Syslog, file monitoring, Socks, Stream, etc., which provides basic support for the analysis of log data at a later stage;
2) Log Parsing, Storage, Retrieval: After the data aggregated into the platform is configured and parsed into a standardized format, it will be systematically stored in distributed clusters and provide users with powerful and flexible retrieval and analysis capabilities;
3) Data Analysis: The platform supports qualitative analysis of data through the use of a powerful rule language and interactive or cyclical execution or real-time execution, so that a variety of threat scenarios, security attack and defense actions can be in the analysis engine and related to the policy rule pairs under the auspices of nothing to hide;
4) Component Integration: The platform has a built-in powerful integration capability that allows docking of external platforms or data through APIs or standard eco-links, making it possible to open up the entire application process and data chain, and improve the overall efficiency of security analysis and disposal;
5) AI Interaction Engine: The platform is embedded with an interactive form of user security analysis based on the LLM model, which allows users to use the model to assist in decision-making and analysis of events and intelligence collection, greatly improving the efficiency and capability of operational handling of security incidents.

5.3 WEB3 AND CHAIN SECURITY DETECTION

Web3 and on-chain security detection is the featured capability of Web3 SOC, which is built based on the NIST Cybersecurity Framework, in which the detection link uses on-chain anomalous behaviour detection, including a multi-blockchain analysis platform, EVM transaction simulation, and machine-learning based smart contract anomaly detection capability, which can provide more sources of on-chain data from Web3 for rapid security response.

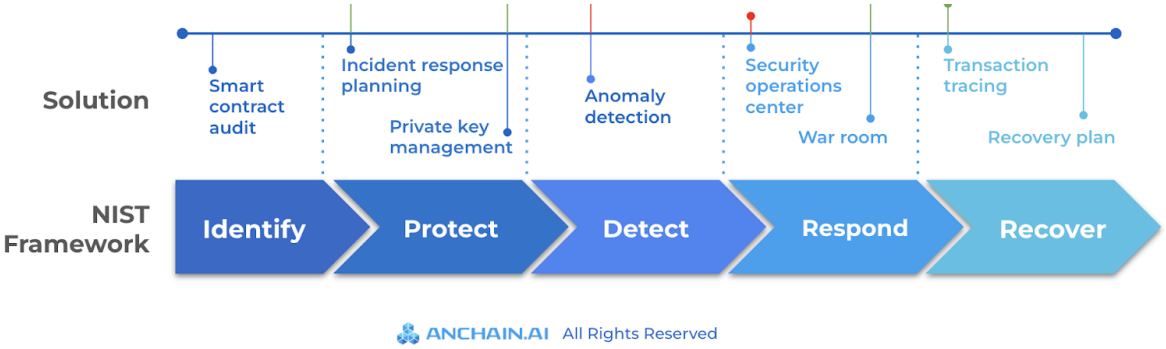

Figure: NIST IPDRR Framework for Web3

- **Identify:** Understand the Web3 digital assets, systems, data, and resources that need to be protected and get a complete picture of the organization's cybersecurity risk profile. For example, a smart contract audit would be appropriate for this phase.
- **Protect:** Implement safeguards to secure critical infrastructure services, prevent or minimize damage caused by cyber threats, and establish security policies and procedures.
- **Detect:** The use of monitoring and detection systems to identify cybersecurity events in a timely manner, enabling early detection and effective response. For example, the use of machine learning to detect fraudulent actors on the Elrond blockchain and to take preventive countermeasures such as blocking transactions falls into this category.
- **Respond:** Develop and implement an incident response plan to resolve detected cybersecurity incidents, minimize damage and ensure a quicker return to normal operations.
- **Recover:** Recovering systems and services impacted by a cybersecurity incident by developing a recovery plan, prioritizing critical functions, and incorporating lessons learned to improve overall resilience. For example, the $100 million worth of cryptocurrency from the Harmony blockchain tracked by the AnChain.AI team falls into this category.

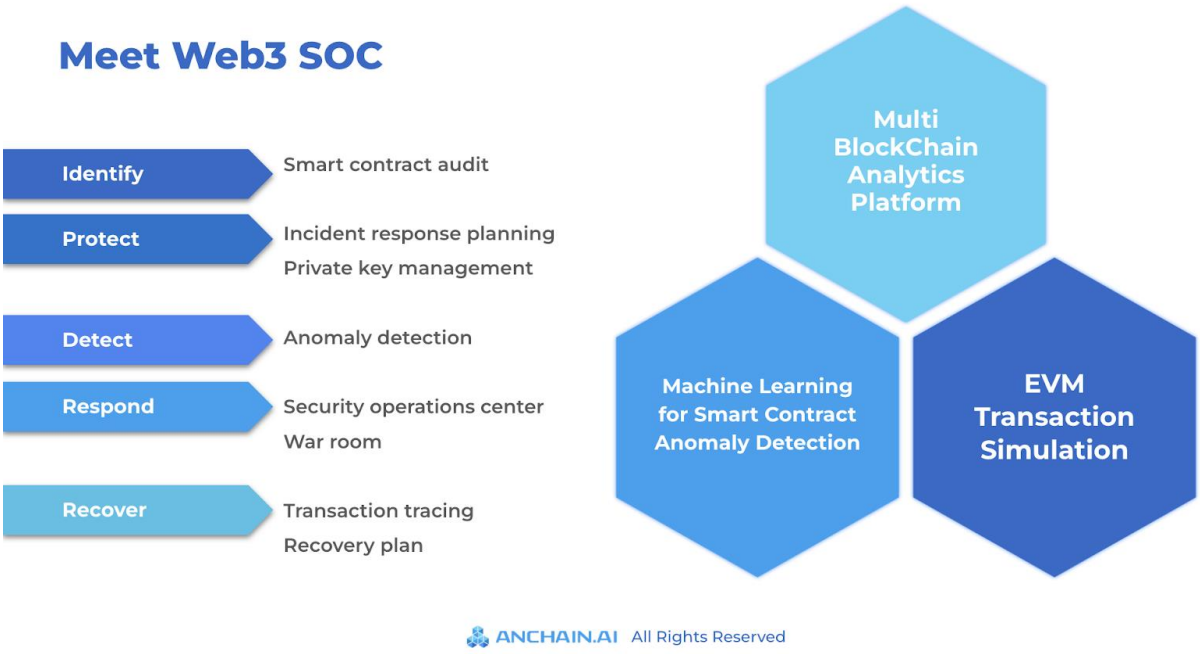

Figure: Meet Web3 SOC

5.4 MANAGED INCIDENT RESPONSE

Managed Event Response (MER) is the last link in Amber Group's security detection and response hosting solution. Amber Group's security engineering team utilizes real-world experience and incident response plans established in advance, combined with SOAR & AI technology, to distribute high-risk events through the event distribution mechanism to the Corresponding event hosting service team, to achieve rapid identification, accurate analysis and timely response to high-risk events.

The core component of managed incident response is the event distribution mechanism, which is responsible for automatically distributing real-time monitored security events to on-duty security analysts and corresponding managed incident service teams based on the type, severity, and time of occurrence of the event, etc. This mechanism improves the efficiency and accuracy of incident response and ensures that each security event is handled by a dedicated team. This distribution mechanism improves the efficiency and accuracy of incident response, ensures that each security alert is handled by a dedicated person, and ensures that each team is able to focus on handling security incidents related to their area of expertise.

During the managed incident response process, SOAR provides critical technical support. SOAR is a technology that integrates security tools and applications to automate response, collaboration, and optimization of security incidents. SOAR technology helps teams to automatically and quickly collect and analyse security incident data, formulate effective response strategies, and automatically execute those strategies to reduce cybersecurity risks. In addition, through SOAR's integration with AI, the Managed Incident Response Service enables intelligent identification,

classification and analysis of unknown and known security events, further improving the speed and accuracy of incident response. In this model, more than 80% of incidents do not require manual intervention by the security team. For incidents that require manual intervention, SOAR and AI can also provide robust technical support, including intelligence integration, environment-based remediation recommendations, summary reports, and more.

Amber Group Managed Incident Response Service Success By combining SOAR and AI technologies, Amber Group can provide customers with efficient and accurate cybersecurity protection solutions.

5.5 SUMMARY OF THE VALUE OF WEB3 MDR SERVICES

Web3 MDR (Managed Detection and Response) service refers to a comprehensive monitoring, detection and response service for enterprise network security. The value of Web3 MDR service not only lies in the fact that it can provide enterprises with highly efficient threat detection and response control capabilities, helping them to detect and handle security threats in a timely manner and strengthen network security protection. In addition, Web3 MDR service is usually provided by professional security teams with rich experience and expertise to analyse and solve security problems more comprehensively. With Web3 MDR service, enterprises can build a **complete, powerful and efficient** security protection and response system in a short period of time, which significantly reduces the overall Mean Time to Detection (MTTD) and Mean Time to Response (MTTR) of the enterprise, reduces security risks and losses, and safeguards business continuity and customer information security, and enhances brand credibility and market competitiveness.

6 WEB3 AND DIGITAL ASSET ON-CHAIN SECURITY SERVICES

The vehicle for virtual assets is blockchain technology, such as Bitcoin, which is the result of bookkeeping by consensus among nodes of a P2P network run by the open-source Bitcoin-Core software. The emergence of Ethereum was further enhanced by the Turing-complete EVM virtual machine that created applications such as ERC20 tokens, NFT, DeFi, and other smart contract-enabled applications. Over the past 10 years, we have witnessed various hacks and considerable financial losses due to problems with the underlying public chain or the implementation of upper layer smart contracts. Even cryptography and private key generation, which are the most basic aspects of blockchain technology, have problems similar to Profanity, Amber Group, based on its 5 years of experience in the blockchain security industry and its security research capabilities, offers the following services: smart contract auditing, on-chain monitoring of funding risks, decentralized protocol monitoring, blockchain node monitoring, incident response and stolen asset tracking. Stolen asset tracking. These services correspond to the time before and after the project start-up, after the unfortunate attack, etc. Amber Group has the corresponding ability and experience to help clients properly deal with the best solution.

Smart Contract Audit Services: Includes basic token contracts, NFT contract vulnerability detection, avoidance of obvious public burn, centralized operation risk, etc. For complex DeFi protocols, such as MakerDAO MCD, SushiSwap, etc., Amber Group team members also have past experience in auditing.

On-chain Monitoring Service for Capital Risk: Amber Group can, through on-chain data tracking, detection and response, on the one hand, identify and dispose of compliance and internal control issues such as non-compliance with the withdrawal of funds from digital currency exchanges and the bypassing of the internal approval process in a timely manner, so as to reduce the compliance risk of the withdrawal of funds and the risk of loss of funds, and at the same time, satisfy the compliance requirements of KYT. On the other hand, it can be based on the blockchain node coverage, real-time listening to transactions on the blockchain, and once the existence of malicious transactions in Mempool is found, the automatic drilling segment program will be launched instantly to grab and run to intercept them, so as to avoid potential losses from arising. To ensure the accuracy and coverage of on-chain monitoring and the effectiveness of responding to unexpected cases, it is necessary to achieve full node coverage of the corresponding blockchain network, including timely detection of node code not upgraded and other potential problems, matching the best synchronization node in order to save resources and so on. In addition, the daily monitoring of some DeFi protocols can also detect some potential vulnerability risks, such as the tampering of Owner's rights, the withdrawal of ultra-large amount of liquidity, and so on.

Incident Response to Security Crisis: Amber Group can analyse and investigate the stolen assets transfer, cross-chain, and coin laundering situation instantly, and notify trading platforms, token issuers, and cooperate with law firms and law enforcement agencies to freeze the funds, collect information about the crime, and assist in the subsequent court proceedings. It should be emphasized that during the incident response phase, some necessary technical interventions can directly intercept hacker attacks and help project owners and users reduce losses, in addition to repairing and upgrading contracts to avoid the spread of collateral damage.

Service Value Summary:

In summary, the Web3 security solution provided by Amber Group can provide customers with full lifecycle Web3 security escort before, during and after the event. Users can access Web3's chained security services in a flexible way to easily enhance Web3 security monitoring, detection and response capabilities for the enterprise's Security Operation Center (SOC). Using the on-chain data analysis capability and on-chain threat intelligence capability we provide, we can minimize the on-chain security risk, abnormal withdrawal risk and bypassing control process risk of digital asset management organizations, and improve the level of internal control of enterprise risk.

AUTHOR TEAM AND ACKNOWLEDGEMENTS

WHITE PAPER STEERING COMMITTEE

Leo Que (Que Yunchuan)
Chief Information Security Officer, Amber Group

Luke Yang
Security & Systems R&D Service Line Leader, Thoughtworks

Betty Shao
Chief Risk Officer, Amber Group

Chiachih Wu
Head of Security Labs / Head of Web3 Security / Web3 Security Industry Leader, Amber Group

Carl Hu (Hu Kaijian)
Head of Information Security Governance, Risk & Compliance / Data Security & Privacy / Data Protection Officer, Amber Group

Steven Zhou
Global Head of Security & Compliance / Head of Security Influence & Communications, Amber Group

Fan Jiang
Technical Principal, Security & Systems R&D Service Line, Thoughtworks

Qian Yan
Technical Principal, Blockchain Specialist, Hong Kong & Macau Market, Thoughtworks

AMBER GROUP TEAM

Guisheng Guo
Security Attack & Defense Expert / Head of GSOC Infrastructure Security

Momo Wang
Virtual Asset Custody Security Specialist / Head of GSOC Digital Wallet Security

Hong Guang (Guang Hong)
Security Operations and Automation Specialist / Head of GSOC Incident Response

Walker Zeng
Head of Application Security & Red Team

Gerry Zhang
Head of Enterprise IT Construction Operations

Juno Sou
Web3 Security Research Specialist

Melvin Hao, Tianxi Hao
Web3 Security Specialist

Yulsa Liu
Security Compliance Specialist

Guski Zhu
Security Compliance Specialist

Eric Yixiao Ge
Risk Manager of Risk Modelling & Data

Xiaokun Xie
Head of Risk Modelling & Data

Cayden Chang
Virtual Asset Compliance Specialist

Serena Wang
Market Development Specialist

Yannie Hui
Market Development Specialist

THOUGHTWORKS TEAM

Yef Zhengyuan Wang
AI Security Specialist

Jing Liu
Cyber Security Specialist

Ash Zeng
Business Security (BizSec) Specialist

SLOWMIST TEAM

Aby Huang
Chief Executive Officer

Zhang Lianfeng
Partner and Chief Information Security Office

BLOCKSEC TEAM

Wu Lei
Co-Founder and Chief Technology Officer

RIGSEC TEAM

Neilson Lei
Chief Technology Officer

ANCHAIN.AI TEAM

Victor Fang
Founder and CEO

ANKURA TEAM

Christopher Marks
Senior Managing Director / APAC D&T Leader

Han Lai
Senior Managing Director / Greater China Leader

Rob Phillips
Senior Managing Director/APAC Cybersecurity Leader

Ryan Rubin
Senior Managing Director / EMEA Cybersecurity and Crypto Expert

Brad Lohmeyer
Senior Managing Director / US Crypto Expert

AMBER | **Building the Future of Digital Assets**

Contact Us
grc@ambergroup.io

www.ambergroup.io