April 15, 2021

Thomson Reuters Institute

Manifest Destiny: Risk, Opportunity & Reward Around Digital Currencies

- Panel: “Zones of Sovereignty”: Is the Future Multichain?

Cybersecurity and Crypto Multichain Platforms

Panelist: Cristina Dolan, Head of Global Alliances RSA NetWitness

An RSA Business

NETWITNESS

“Zones of Sovereignty”: Is the Future Multichain?

Panelist: Cristina Dolan, Head of Global Alliances RSA NetWitness

For years, blockchain has thrived on its enhanced security protocols and transactional integrity. Yet in the wake of significant breaches in the cross-chain protocol Poly Network and Wormhole Bridge, pointed questions over the inherent vulnerabilities of blockchain platforms suggest profound and fundamental changes ahead. As Ethereum inventor Vitalik Buterin presciently warned, cross-chain ecosystems, while not without their merits, are always already at greater risk than, say, bridges with multi-chain security, a platform whose intrinsic protocol rules could help theoretically curtail “systemic contagion.” This conversation explores the future of blockchain security. Is the crypto industry sufficiently prepared for the next incursion?

An RSA Business

Cybersecurity and Blockchain Ecosystems

Facets of Cyber Security for Blockchain Enabled Ecosystems

- **TOPICS:**
  - Multichains and Bridges
    - What are Multichains and Bridges?
    - What role do Multichains and Bridges play?
  - What Vulnerabilities are introduced by Multichains and Bridges?
    - Recent Hacks
    - Why are Financial DeFi applications vulnerable?
    - How are the vulnerabilities similar or different from traditional financial platforms?
  - Cyber Security for the Entire Ecosystem
    - Surface Area of Ecosystem
    - Vulnerabilities of Components
      - Blockchain
  - Regulatory Requirement for Active Managed Detect and Response

Cybersecurity and Blockchain Ecosystems

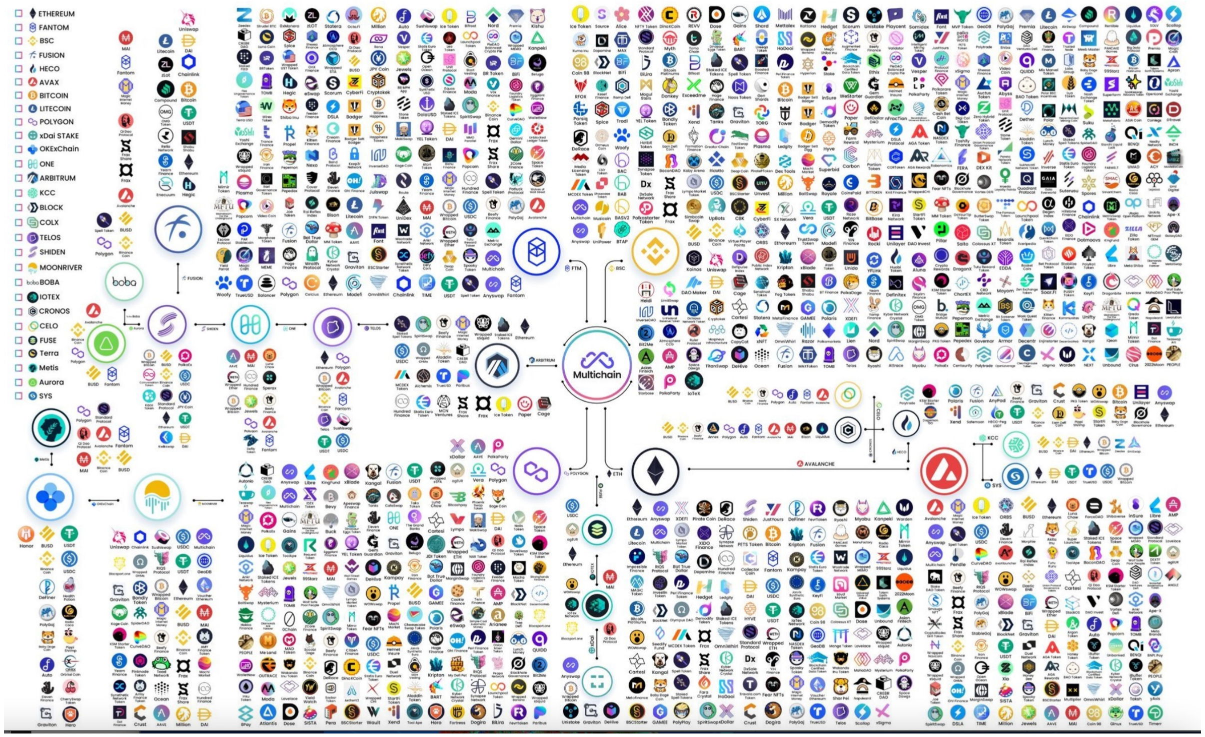
MultiChains and Bridges

- **What are Multichains and Bridges?**
  - Complex world of Siloed Blockchains has been expanded through the use of Multichain and Bridges.
  - Today there are many Layer 1 and Layer 2 protocol blockchains.
  - Multichain:
    - Through the uses of bridges, Multichain allows and asset on one chain to be sent to another chain.
  - Bridge:
    - Connects two blockchains and are a foundational part of Multichain

Cybersecurity and Blockchain Ecosystems

Map of MultiChains, Bridges and Connected Blockchains

- This complex map shows Multichain, bridges and many of the blockchain token networks they connect.
- Check out the following link for a detailed view: https://pbs.twimg.com/media/FJTAQyoXIAEXM_w?format=jpg&name=large



Cybersecurity and Blockchain Ecosystems

MultiChains and Bridges

- **What role do Multichain and Bridges Plan?**
  - Interoperability is a requirement for the growth of blockchain ecosystems, especially financial networks.
  - Each blockchain is a silo and they don't have *native* interoperability with other blockchains.
  - ***Blockchain Bridges***, also known as ***Cross-Bridge Blockchains*** *or* ***Cross-Chain Bridges***, provide the interoperability between different blockchains.
    - Enable the transfer of tokens, smart contracts, assets or data between two independent blockchains.
      - An example would be the ability to take bitcoin and spend it on Ethereum through a bridge.
      - Both bitcoin and Ethereum are very popular, although they have very different protocols and governance rules.
      - Without Multichain and bridges, transfer from one blockchain to another would require many fees.
      - Communications across different blockchains can be enabled without involving intermediaries
    - Help decrease congestion and high transaction costs.
    - Offers a neutral conduit enabling a smooth transition between multiple blockchains, and this conduit is not dependent on a specific blockchain.
    - Tokens on one blockchain network are 'wrapped' so that they can represent value on a different network.
      - Wrapped coins are represented by a reserve of cryptocurrency to underwrite the cross-network transaction values
  - *Distributed Finance* and *Gaming* are popular use cases for Multichain and Bridges

Cybersecurity and Blockchain Ecosystems

What Vulnerabilities are introduced by MultiChains and Bridges?

- Recent Hacks:
  - Ronin Bridge – $540M in Ethereum and USDC Stablecoin
  - Qubit Bridge – $80M in Crypto
  - Wormhold Bridge – $320M in Crypto
  - Meter.io Bridge - $4.2M in Crypto
  - Poly Network - $611M in Crypto – although funds were returned

Cybersecurity and Blockchain Ecosystems

What Vulnerabilities are introduced by MultiChains and Bridges?

- Why are Financial DeFi applications vulnerable?
  - DeFi (Decentralized Finance) utilize distributed ledgers to offer financial instruments without relying on intermediaries (although many DeFi solutions have centralized governance and management)
  - The centralization of value makes DeFi solutions a target for hackers due to the high concentration of value.
  - The DeFi algorithms often represent vulnerabilities that hackers can manipulate in unintended ways when executing the lending, borrowing or creation of synthetic assets on the platforms. Flash loan attacks or manipulation of data ingested by the oracles that feed smart contracts are just examples of manipulation.
  - Multichain or bridge networks require parking collateral when wrapping the crypto assets for use across different networks. These large reserve pools of cryptocurrencies are very attractive to hackers.
  - DeFi requires a large number of ‘independent’ blockchain network nodes to avoid market manipulation. The utilization of Ethereum or other large blockchain networks for ‘secure governance’ can provide the required security. Some smaller networks lack the appropriate number of independent validators that prevent manipulation.

Cybersecurity and Blockchain Ecosystems

What Vulnerabilities are introduced by MultiChains and Bridges?

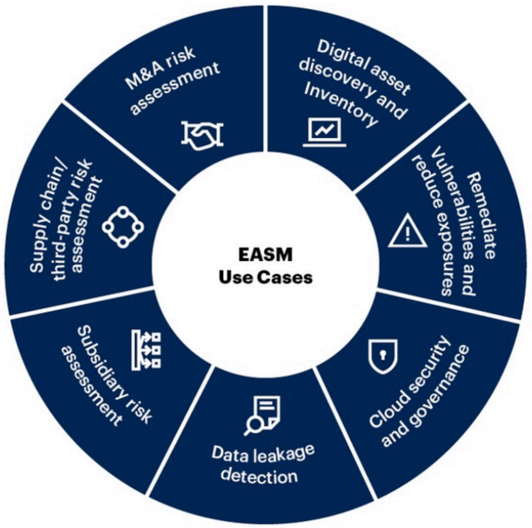
- How are the vulnerabilities similar or different from traditional financial platforms?
  - All financial ecosystems have vulnerabilities and understanding the risks is and important first step
  - Many blockchain and crypto platforms are less mature and tend to have less focus on cybersecurity
    - The recent Ronin hack involved '*traditional social engineering attack*' in addition to security design issues.
    - The protection of private keys requires the implementation of cybersecurity protocols that protect from social engineering penetrations.
    - Many crypto platforms do not have active cyber security management to actively detect and respond to activities on the network. This is a critical requirement for cyber insurance coverage and regulatory compliance.
  - DeFi and other blockchain enabled crypto platforms have the same requirements that regulators have placed on traditional financially focused organizations.
  - Cyber Insurance for financial platforms requires active cyber security management.

Cybersecurity and Blockchain Ecosystems

Cyber Security for the Entire Ecosystem

- Surface Area of the Ecosystem
  - Understanding the External Attack Surface is an initial step
  - The chart to the right is from a Gartner Report.
  - Traditional Cybersecurity approaches apply for digital asset ecosystems

Common Use Cases for External Attack Surface Management


EASM
Use Cases
M&A risk assessment
Digital asset discovery and Inventory
Remediate Vulnerabilities and reduce exposures
Cloud security and governance
Data leakage detection
Subsidiary risk assessment
Supply chain/ third-party risk assessment

Source: Gartner
737807_C

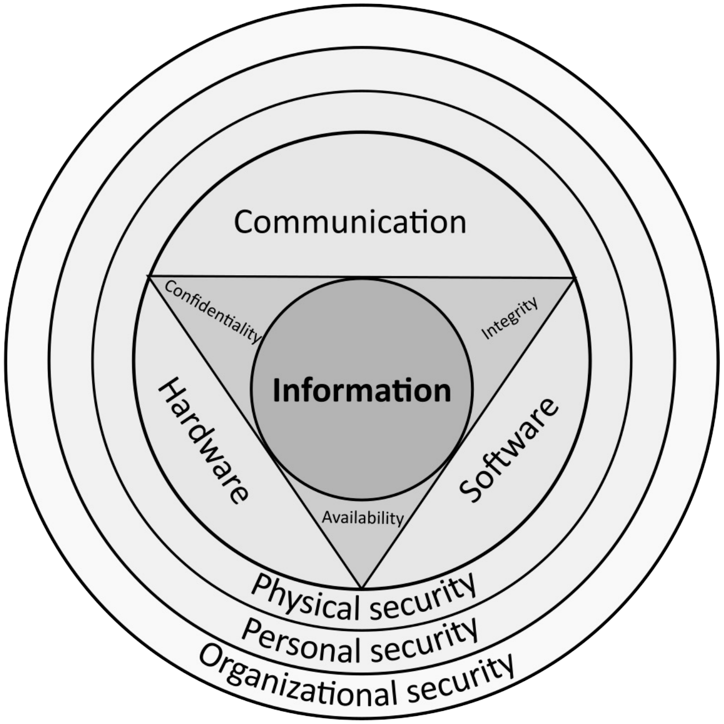
Gartner

NETWITNESS

Cybersecurity and Blockchain Ecosystems

Cyber Security for the Entire Ecosystem

- Vulnerabilities of Components
  - Blockchain (Subset of Vulnerabilities)
    - Loss of Private Keys
    - Wallet Credential Theft (Phishing)
    - Social Engineering
    - Exchanges
    - Smart contracts
    - Mining Pool Attacks
    - Transaction verification mechanism attacks
    - Distributed Denial of Service (DDoS)
    - Algorithm Flaws in DeFi and other financial applications



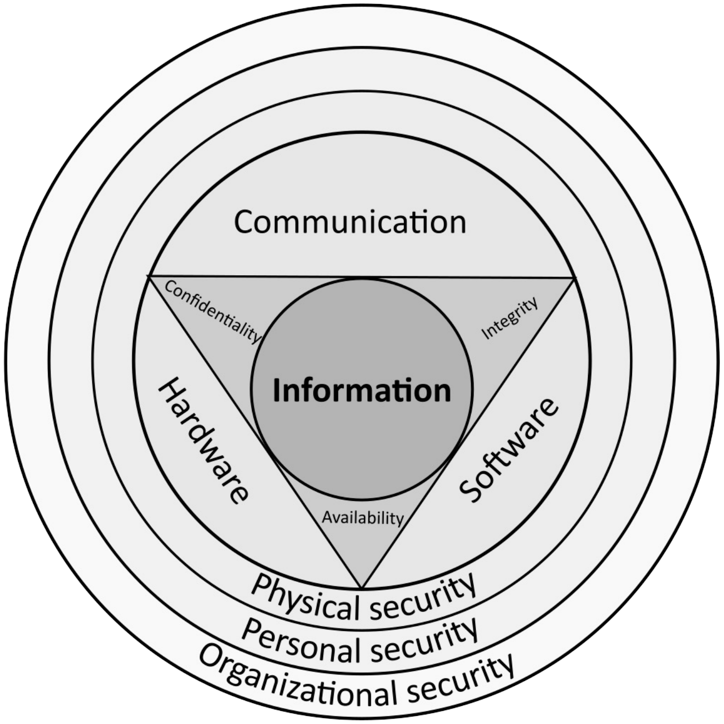
Vulnerabilities in Information Security

https://en.wikipedia.org/wiki/Vulnerability_(computing)

Cybersecurity and Blockchain Ecosystems

Cyber Security for the Entire Ecosystem

- Vulnerabilities of Components
  - Traditional Financial Systems
    - Blockchain is a component of a networked financial platform
    - Complexity of networked financial systems has grown
    - Cloud environments, APIs, Containers and other components of financial applications represent cyber security risks
    - As more applications have moved into the cloud, new vulnerabilities have evolved.

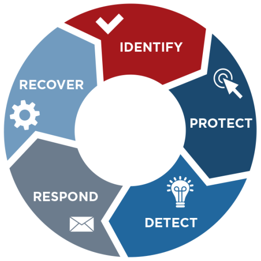


Vulnerabilities in Information Security

https://en.wikipedia.org/wiki/Vulnerability_(computing)

Cybersecurity and Blockchain Ecosystems

NIST (National Institute of Standard and Technology (NIST)



1 IDENTIFY

Identify and control who has access to your business information

Conduct background checks

Require individual user accounts for each employee

Create policies and procedures for cybersecurity

2 PROTECT

Limit employee access to data and information

Install Surge Protectors and Uninterruptible Power Supplies (UPS)

Patch your operating systems and applications routinely

Install and activate software and hardware firewalls on all your business networks

Secure your wireless access point and networks

Set up web and email filters

Use encryption for sensitive business information

Dispose of old computers and media safely

Train your employees

3 DETECT

Install and update anti-virus, anti-spyware, and other anti-malware programs

Maintain and monitor logs

4 RESPOND

Develop a plan for disasters and information security incidents

5 RECOVER

Make full backups of important business data and information

Continue to schedule incremental backups

Consider cyber insurance

Make improvements to processes/ procedures/ technologies

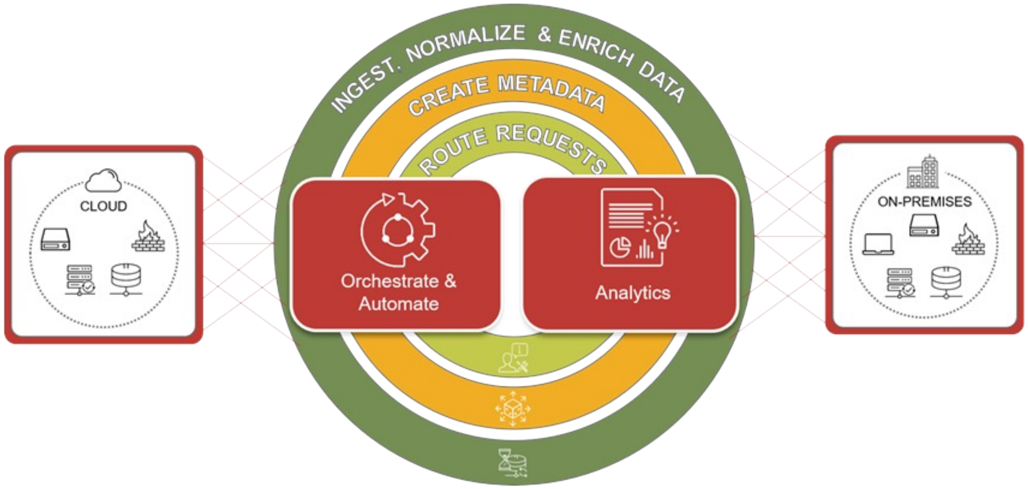
- NIST is the standard for cybersecurity for ‘all’ systems including blockchain enabled fintechs.
- All platforms must recognize the threat of cyber attacks and implement plants to prevent them.
- Understanding vulnerabilities is a critical first step.
- Gartner’s Guide for Managed Detect and Response (MDR) states that by 2025, 50% of companies will be using MDR for threat monitoring, detection and response.

Cybersecurity and Blockchain Ecosystems

MDR – Managed Detection and Response and Adjacent Services

- Garter claims that by 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities

RSA NetWitness Platform for XDR is designed to maximize speed and efficiency of threat detection and response by cumulating data from multiple sources, normalizing and enriching it, and presenting clear information to the user and taking direct action when defined.



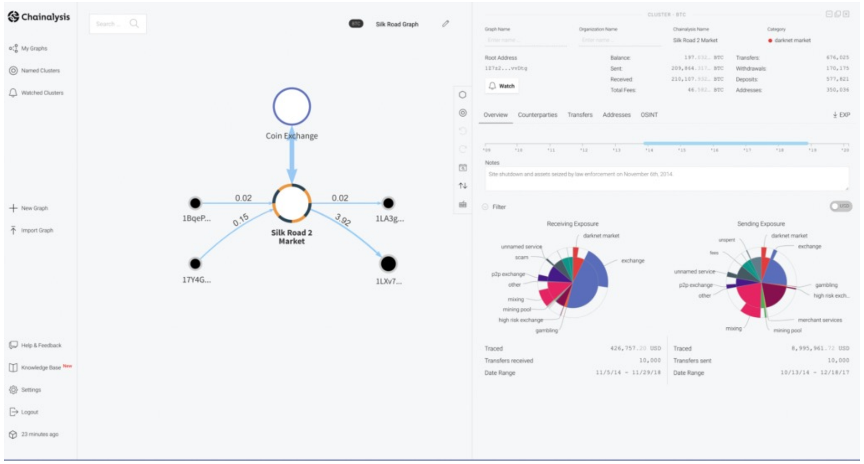
Cybersecurity and Blockchain Ecosystems

Regulators and Compliance Software Solutions for Blockchain Platforms

- Cryptocurrency Compliance, Forensics and Surveillance Solutions
  - Chainalysis
  - Elliptic
  - CipherTrace
  - Anchain.ai
  - Crystal Blockchain
  - Confirm
  - Certik

- Services
  - Anti-Money Laundering
  - KYC – Know Your Customer
  - Know Your Transaction – Crypto Transaction Monitoring
  - Travel Rule for VASP (Virtual Asset Service Providers)
  - VASP Screening
  - Crypto Wallet Screening
  - Financial Investigations – criminal activity, fraud and sanctions.

Chainalysis Reactor Screen



Graph Name: Enter name ...
Organization Name: Enter name ...
Chainalysis Name: Silk Road 2 Market
Category: ● darknet market

Root Address: 127z2...vvDtg

Balance:	197.032.. BTC	Transfers:	676,025
Sent:	209,864.317.. BTC	Withdrawals:	170,175
Received:	210,107.932.. BTC	Deposits:	577,821
Total Fees:	46.582.. BTC	Addresses:	350,036

Notes: Site shutdown and assets seized by law enforcement on November 6th, 2014.

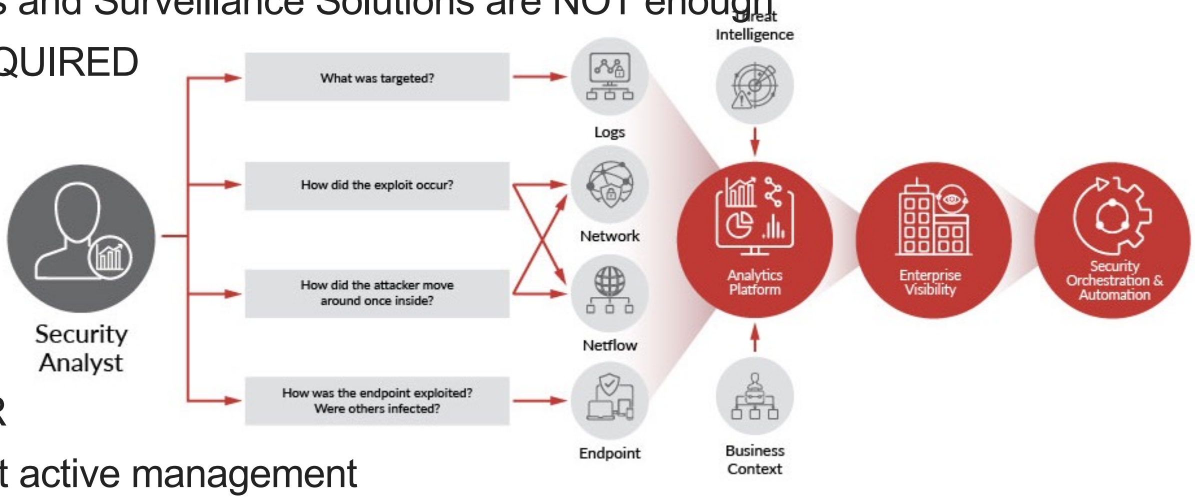
Traced	426,757.20 USD	Traced	8,995,961.72 USD
Transfers received	10,000	Transfers sent	10,000
Date Range	11/5/14 - 11/29/18	Date Range	10/13/14 - 12/18/17

https://blockcrunch.co/2021/07/02/top-blockchain-analysis-and-surveillance-tools/

Cybersecurity and Blockchain Ecosystems

Blockchain Platforms Require Cybersecurity Operations

- Blockchain Platforms and Echo Systems Require Sophisticated Security Operations Centers
  - Cryptocurrency Compliance, Forensics and Surveillance Solutions are NOT enough
  - Managed Detect and Response is REQUIRED
  - Incident Response Plans REQUIRED
  - Regulatory Requirements:
    - Report Hacks/Breaches
    - Report Data Loss
- Required Managed Cyber Security
  - Cyber Insurance requires Active MDR
  - Insurance doesn't reduce risk, without active management
  - Regulators, Insurance Firms and Courts will require demonstrated active management by FinTechs – regardless of underlying technology used
  - Blockchain enabled platforms are complex networked FinTech solutions that require MDR


Security Analyst
What was targeted?
How did the exploit occur?
How did the attacker move around once inside?
How was the endpoint exploited? Were others infected?
Logs
Network
Netflow
Endpoint
Threat Intelligence
Analytics Platform
Business Context
Enterprise Visibility
Security Orchestration & Automation

> “Cybersecurity is the most immediate, financially material sustainability and ESG risk that organizations face today.”

Cristina Dolan, Head of Global Alliances, NetWitness

NETWITNESS
An RSA Business

NETWITNESS

April 15, 2021

Thomson Reuters Institute

Manifest Destiny: Risk, Opportunity & Reward Around Digital Currencies

- Panel: “Zones of Sovereignty”: Is the Future Multichain?

Cybersecurity and Crypto Multichain Platforms

Panelist: Cristina Dolan, Head of Global Alliances RSA NetWitness