

Blockchain in Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Software Solutions and Services), Security Type (Private Blockchain, Public Blockchain and Hybrid Blockchain), Platform, Organization Size, Deployment Mode, Application, End User and By Geography

<https://marketpublishers.com/r/BE197F86A3E0EN.html>

Date: July 2025

Pages: 150

Price: US\$ 4,150.00 (Single User License)

ID: BE197F86A3E0EN

Abstracts

According to Statistics MRC, the Global Blockchain in Cybersecurity Market is accounted for \$123.0 billion in 2025 and is expected to reach \$1270.7 billion by 2032 growing at a CAGR of 39.6% during the forecast period. Blockchain in cybersecurity is the application of decentralized ledger technology to enhance data integrity, transparency, and resilience against cyber threats. By storing information across distributed nodes and using cryptographic hashing, blockchain mitigates risks of tampering, unauthorized access, and single-point failures. It is increasingly used for identity verification, secure data sharing, and transaction authentication. The immutability and traceability of blockchain records support robust security frameworks across sectors, bolstering trust in critical systems and digital infrastructures.

According to study on blockchain-based cybersecurity systems, implementing decentralized, immutable ledgers enabled secure sharing of threat intelligence ensuring all interactions were verifiable and traceable, thereby mitigating insider threats and improving collaborative defense.

Market Dynamics:

Driver:

Demand for enhanced data integrity and transparency

Blockchain's immutable ledger capabilities offer a transparent framework where every transaction is recorded and traceable, reducing the scope for unauthorized alterations. As businesses prioritize regulatory compliance and audit readiness, blockchain provides a trusted mechanism for data validation across networks. Enterprises are recognizing its utility in authenticating access credentials and securing sensitive records. The rising demand for decentralized identity verification and verifiable data exchange is propelling blockchain adoption in cybersecurity.

Restraint:

High implementation costs and resource intensive nature

Organizations must overhaul existing legacy systems to accommodate decentralized architectures, often requiring custom development. The cost of infrastructure, including node deployment and network scalability, presents a barrier for small and mid-sized enterprises. Moreover, onboarding skilled professionals to manage blockchain environments adds to operational expenses. Energy consumption, especially in public blockchains, has further raised concerns around sustainability and feasibility in enterprise security settings.

Opportunity:

Decentralized secure data storage and audit trails

Blockchain's distributed ledger framework enables secure data storage without reliance on centralized servers, minimizing vulnerabilities from single-point failures. The technology creates detailed audit trails that log every system interaction, enhancing visibility and accountability. Such capabilities are crucial in sectors handling sensitive information, including healthcare, finance, and government. Advanced consensus protocols ensure only verified transactions are recorded, improving the accuracy and trustworthiness of cybersecurity systems.

Threat:

Private key management and human error

Loss, theft, or mismanagement of private keys can result in irreversible data breaches

or asset access failures. Human error, such as poor key storage or incorrect configuration, may compromise an otherwise secure system. There's also growing concern around phishing tactics designed to steal credentials in decentralized environments. Without robust identity recovery mechanisms, blockchain-based cybersecurity platforms face risk exposure that traditional systems may mitigate differently.

Covid-19 Impact:

The pandemic accelerated the digitalization of enterprise operations, prompting a surge in cybersecurity demand and a re-evaluation of existing frameworks. Remote work setups exposed gaps in traditional security models, driving interest in blockchain's decentralized approach. However, resource diversion during COVID-19 delayed blockchain integration projects in several sectors. The need for resilient and traceable security protocols became evident, pushing blockchain back into strategic roadmaps.

The software solutions segment is expected to be the largest during the forecast period

The software solutions segment is expected to account for the largest market share during the forecast period due to their scalability and ease of deployment. These solutions manage encryption, data validation, and identity authentication without requiring extensive hardware modifications. Vendors are building modular platforms that can integrate with existing IT infrastructure while delivering blockchain's core benefits. Customizable dashboards, analytics tools, and API-driven frameworks enhance monitoring and threat detection capabilities.

The distributed ledger technology (DLT) platforms segment is expected to have the highest CAGR during the forecast period

Over the forecast period, the distributed ledger technology (DLT) platforms segment is predicted to witness the highest growth rate owing to the platforms offer robust architectures for secure peer-to-peer communication, document verification, and access control. Innovations in consensus algorithms and scalability solutions are making DLT more enterprise-friendly. Businesses are leveraging platforms to build permission ecosystems where data can be shared across departments or partners with traceability and security.

Region with largest share:

During the forecast period, the Asia Pacific region is expected to hold the largest market share due to substantial investments in blockchain research and development.

Governments and enterprises in the region are rolling out pilot projects to secure digital infrastructure against cyber threats. Countries like China, India, and South Korea are implementing blockchain in public services, finance, and telecom sectors. The region's dynamic startup ecosystem and favorable regulatory initiatives are supporting market maturity.

Region with highest CAGR:

Over the forecast period, the North America region is anticipated to exhibit the highest CAGR due to the region benefits from a concentration of tech giants, mature digital ecosystems, and regulatory clarity. Cybersecurity startups are rapidly adopting blockchain to enhance service portfolios, especially in cloud security and identity verification. U.S. federal agencies and financial institutions are exploring blockchain for secure data management and fraud detection. With ongoing digital transformation and proactive threat mitigation efforts, North America remains a fertile ground for blockchain innovation in cybersecurity.

Key players in the market

Some of the key players in Blockchain in Cybersecurity Market include IBM, Trail of Bits, SlowMist, SAP, Quantstamp, Oracle, OpenZeppelin, Microsoft, Hewlett Packard Enterprise (HPE), Halborn, Guardtime, Empirica S.A., Digital Asset Holdings, Cyber Infrastructure Pvt. Ltd., CertiK, BlockSec, Bitfury Group and Accenture.

Key Developments:

In July 2025, IBM launched its new Power11 data center chips and servers, offering energy efficiency and near-zero planned software downtime. The Power11 line includes advanced ransomware detection (within a minute) and aims to simplify AI deployment with integrated software chip design.

In June 2025, Oracle and AMD announced a collaboration to offer Instinct MI355X GPU clusters on Oracle Cloud Infrastructure, enabling zettascale AI workloads. OCI users can access high-density AI training and inference capacity up to 131,072 MI355X GPUs with improved price-performance.

In April 2025, Accenture announced the Brainstorm AI 2025 series of global

conferences, scheduled for London. Brainstorm AI highlights Accenture's position at the forefront of enabling AI transformation.

Components Covered:

Software Solutions

Services

Security Types Covered:

Private Blockchain

Public Blockchain

Hybrid Blockchain

Platforms Covered:

Blockchain-as-a-Service (BaaS)

Distributed Ledger Technology (DLT) Platforms

Cryptographic Platforms

Other Platforms

Organization Sizes Covered:

Small and Medium-sized Enterprises (SMEs)

Large Enterprises

Deployment Modes Covered:

On-premise

Cloud-based

Hybrid

Applications Covered:

Identity Management

Data Security & Integrity

Secure Communication

Distributed Denial of Service (DDoS) Protection

IoT Security

Supply Chain Security & Traceability

Smart Contract Security

Fraud Detection & Prevention

Other Applications

End Users Covered:

Banking, Financial Services, and Insurance (BFSI)

IT & Telecommunication

Healthcare & Life Sciences

Government & Public Sector

Retail & E-commerce

Manufacturing

Transportation & Logistics

Other End Users

Regions Covered:

North America

US

Canada

Mexico

Europe

Germany

UK

Italy

France

Spain

Rest of Europe

Asia Pacific

Japan

China

India

Australia

New Zealand

South Korea

Rest of Asia Pacific

South America

Argentina

Brazil

Chile

Rest of South America

Middle East & Africa

Saudi Arabia

UAE

Qatar

South Africa

Rest of Middle East & Africa

What our report offers:

- Market share assessments for the regional and country-level segments
- Strategic recommendations for the new entrants
- Covers Market data for the years 2024, 2025, 2026, 2028, and 2032
- Market Trends (Drivers, Constraints, Opportunities, Threats, Challenges, Investment Opportunities, and recommendations)
- Strategic recommendations in key business segments based on the market

estimations

- Competitive landscaping mapping the key common trends
- Company profiling with detailed strategies, financials, and recent developments
- Supply chain trends mapping the latest technological advancements

Free Customization Offerings:

All the customers of this report will be entitled to receive one of the following free customization options:

Company Profiling

Comprehensive profiling of additional market players (up to 3)

SWOT Analysis of key players (up to 3)

Regional Segmentation

Market estimations, Forecasts and CAGR of any prominent country as per the client's interest (Note: Depends on feasibility check)

Competitive Benchmarking

Benchmarking of key players based on product portfolio, geographical presence, and strategic alliance

Contents

1 EXECUTIVE SUMMARY

2 PREFACE

- 2.1 Abstract
- 2.2 Stake Holders
- 2.3 Research Scope
- 2.4 Research Methodology
 - 2.4.1 Data Mining
 - 2.4.2 Data Analysis
 - 2.4.3 Data Validation
 - 2.4.4 Research Approach
- 2.5 Research Sources
 - 2.5.1 Primary Research Sources
 - 2.5.2 Secondary Research Sources
 - 2.5.3 Assumptions

3 MARKET TREND ANALYSIS

- 3.1 Introduction
- 3.2 Drivers
- 3.3 Restraints
- 3.4 Opportunities
- 3.5 Threats
- 3.6 Application Analysis
- 3.7 End User Analysis
- 3.8 Emerging Markets
- 3.9 Impact of Covid-19

4 PORTERS FIVE FORCE ANALYSIS

- 4.1 Bargaining power of suppliers
- 4.2 Bargaining power of buyers
- 4.3 Threat of substitutes
- 4.4 Threat of new entrants
- 4.5 Competitive rivalry

5 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY COMPONENT

- 5.1 Introduction
- 5.2 Software Solutions
 - 5.2.1 Platforms
 - 5.2.2 Identity & Access Management (IAM) Solutions
 - 5.2.3 Key Management Solutions
 - 5.2.4 Data Security & Privacy Solutions
 - 5.2.5 Smart Contract Security Tools
 - 5.2.6 Threat Intelligence Platforms
 - 5.2.7 Secure Communication Solutions
 - 5.2.8 Blockchain Security Audits & Analytics
- 5.3 Services
 - 5.3.1 Advisory & Consulting Services
 - 5.3.2 Deployment & Integration Services
 - 5.3.3 Support & Maintenance Services
 - 5.3.4 Training & Education

6 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY SECURITY TYPE

- 6.1 Introduction
- 6.2 Private Blockchain
- 6.3 Public Blockchain
- 6.4 Hybrid Blockchain

7 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY PLATFORM

- 7.1 Introduction
- 7.2 Blockchain-as-a-Service (BaaS)
- 7.3 Distributed Ledger Technology (DLT) Platforms
- 7.4 Cryptographic Platforms
- 7.5 Other Platforms

8 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY ORGANIZATION SIZE

- 8.1 Introduction
- 8.2 Small and Medium-sized Enterprises (SMEs)
- 8.3 Large Enterprises

9 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY DEPLOYMENT MODE

- 9.1 Introduction
- 9.2 On-premise
- 9.3 Cloud-based
- 9.4 Hybrid

10 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY APPLICATION

- 10.1 Introduction
- 10.2 Identity Management
- 10.3 Data Security & Integrity
- 10.4 Secure Communication
- 10.5 Distributed Denial of Service (DDoS) Protection
- 10.6 IoT Security
- 10.7 Supply Chain Security & Traceability
- 10.8 Smart Contract Security
- 10.9 Fraud Detection & Prevention
- 10.10 Other Applications

11 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY END USER

- 11.1 Introduction
- 11.2 Banking, Financial Services, and Insurance (BFSI)
- 11.3 IT & Telecommunication
- 11.4 Healthcare & Life Sciences
- 11.5 Government & Public Sector
- 11.6 Retail & E-commerce
- 11.7 Manufacturing
- 11.8 Transportation & Logistics
- 11.9 Other End Users

12 GLOBAL BLOCKCHAIN IN CYBERSECURITY MARKET, BY GEOGRAPHY

- 12.1 Introduction
- 12.2 North America
 - 12.2.1 US

- 12.2.2 Canada
- 12.2.3 Mexico
- 12.3 Europe
 - 12.3.1 Germany
 - 12.3.2 UK
 - 12.3.3 Italy
 - 12.3.4 France
 - 12.3.5 Spain
 - 12.3.6 Rest of Europe
- 12.4 Asia Pacific
 - 12.4.1 Japan
 - 12.4.2 China
 - 12.4.3 India
 - 12.4.4 Australia
 - 12.4.5 New Zealand
 - 12.4.6 South Korea
 - 12.4.7 Rest of Asia Pacific
- 12.5 South America
 - 12.5.1 Argentina
 - 12.5.2 Brazil
 - 12.5.3 Chile
 - 12.5.4 Rest of South America
- 12.6 Middle East & Africa
 - 12.6.1 Saudi Arabia
 - 12.6.2 UAE
 - 12.6.3 Qatar
 - 12.6.4 South Africa
 - 12.6.5 Rest of Middle East & Africa

13 KEY DEVELOPMENTS

- 13.1 Agreements, Partnerships, Collaborations and Joint Ventures
- 13.2 Acquisitions & Mergers
- 13.3 New Product Launch
- 13.4 Expansions
- 13.5 Other Key Strategies

14 COMPANY PROFILING

- 14.1 IBM
- 14.2 Trail of Bits
- 14.3 SlowMist
- 14.4 SAP
- 14.5 Quantstamp
- 14.6 Oracle
- 14.7 OpenZeppelin
- 14.8 Microsoft
- 14.9 Hewlett Packard Enterprise (HPE)
- 14.10 Halborn
- 14.11 Guardtime
- 14.12 Empirica S.A.
- 14.13 Digital Asset Holdings
- 14.14 Cyber Infrastructure Pvt. Ltd.
- 14.15 CertiK
- 14.16 BlockSec
- 14.17 Bitfury Group
- 14.18 Accenture

List Of Tables

LIST OF TABLES

Table 1 Global Blockchain in Cybersecurity Market Outlook, By Region (2024-2032) (\$MN)

Table 2 Global Blockchain in Cybersecurity Market Outlook, By Component (2024-2032) (\$MN)

Table 3 Global Blockchain in Cybersecurity Market Outlook, By Software Solutions (2024-2032) (\$MN)

Table 4 Global Blockchain in Cybersecurity Market Outlook, By Platforms (2024-2032) (\$MN)

Table 5 Global Blockchain in Cybersecurity Market Outlook, By Identity & Access Management (IAM) Solutions (2024-2032) (\$MN)

Table 6 Global Blockchain in Cybersecurity Market Outlook, By Key Management Solutions (2024-2032) (\$MN)

Table 7 Global Blockchain in Cybersecurity Market Outlook, By Data Security & Privacy Solutions (2024-2032) (\$MN)

Table 8 Global Blockchain in Cybersecurity Market Outlook, By Smart Contract Security Tools (2024-2032) (\$MN)

Table 9 Global Blockchain in Cybersecurity Market Outlook, By Threat Intelligence Platforms (2024-2032) (\$MN)

Table 10 Global Blockchain in Cybersecurity Market Outlook, By Secure Communication Solutions (2024-2032) (\$MN)

Table 11 Global Blockchain in Cybersecurity Market Outlook, By Blockchain Security Audits & Analytics (2024-2032) (\$MN)

Table 12 Global Blockchain in Cybersecurity Market Outlook, By Services (2024-2032) (\$MN)

Table 13 Global Blockchain in Cybersecurity Market Outlook, By Advisory & Consulting Services (2024-2032) (\$MN)

Table 14 Global Blockchain in Cybersecurity Market Outlook, By Deployment & Integration Services (2024-2032) (\$MN)

Table 15 Global Blockchain in Cybersecurity Market Outlook, By Support & Maintenance Services (2024-2032) (\$MN)

Table 16 Global Blockchain in Cybersecurity Market Outlook, By Training & Education (2024-2032) (\$MN)

Table 17 Global Blockchain in Cybersecurity Market Outlook, By Security Type (2024-2032) (\$MN)

Table 18 Global Blockchain in Cybersecurity Market Outlook, By Private Blockchain

(2024-2032) (\$MN)

Table 19 Global Blockchain in Cybersecurity Market Outlook, By Public Blockchain (2024-2032) (\$MN)

Table 20 Global Blockchain in Cybersecurity Market Outlook, By Hybrid Blockchain (2024-2032) (\$MN)

Table 21 Global Blockchain in Cybersecurity Market Outlook, By Platform (2024-2032) (\$MN)

Table 22 Global Blockchain in Cybersecurity Market Outlook, By Blockchain-as-a-Service (BaaS) (2024-2032) (\$MN)

Table 23 Global Blockchain in Cybersecurity Market Outlook, By Distributed Ledger Technology (DLT) Platforms (2024-2032) (\$MN)

Table 24 Global Blockchain in Cybersecurity Market Outlook, By Cryptographic Platforms (2024-2032) (\$MN)

Table 25 Global Blockchain in Cybersecurity Market Outlook, By Other Platforms (2024-2032) (\$MN)

Table 26 Global Blockchain in Cybersecurity Market Outlook, By Organization Size (2024-2032) (\$MN)

Table 27 Global Blockchain in Cybersecurity Market Outlook, By Small and Medium-sized Enterprises (SMEs) (2024-2032) (\$MN)

Table 28 Global Blockchain in Cybersecurity Market Outlook, By Large Enterprises (2024-2032) (\$MN)

Table 29 Global Blockchain in Cybersecurity Market Outlook, By Deployment Mode (2024-2032) (\$MN)

Table 30 Global Blockchain in Cybersecurity Market Outlook, By On-premise (2024-2032) (\$MN)

Table 31 Global Blockchain in Cybersecurity Market Outlook, By Cloud-based (2024-2032) (\$MN)

Table 32 Global Blockchain in Cybersecurity Market Outlook, By Hybrid (2024-2032) (\$MN)

Table 33 Global Blockchain in Cybersecurity Market Outlook, By Application (2024-2032) (\$MN)

Table 34 Global Blockchain in Cybersecurity Market Outlook, By Identity Management (2024-2032) (\$MN)

Table 35 Global Blockchain in Cybersecurity Market Outlook, By Data Security & Integrity (2024-2032) (\$MN)

Table 36 Global Blockchain in Cybersecurity Market Outlook, By Secure Communication (2024-2032) (\$MN)

Table 37 Global Blockchain in Cybersecurity Market Outlook, By Distributed Denial of Service (DDoS) Protection (2024-2032) (\$MN)

Table 38 Global Blockchain in Cybersecurity Market Outlook, By IoT Security (2024-2032) (\$MN)

Table 39 Global Blockchain in Cybersecurity Market Outlook, By Supply Chain Security & Traceability (2024-2032) (\$MN)

Table 40 Global Blockchain in Cybersecurity Market Outlook, By Smart Contract Security (2024-2032) (\$MN)

Table 41 Global Blockchain in Cybersecurity Market Outlook, By Fraud Detection & Prevention (2024-2032) (\$MN)

Table 42 Global Blockchain in Cybersecurity Market Outlook, By Other Applications (2024-2032) (\$MN)

Table 43 Global Blockchain in Cybersecurity Market Outlook, By End User (2024-2032) (\$MN)

Table 44 Global Blockchain in Cybersecurity Market Outlook, By Banking, Financial Services, and Insurance (BFSI) (2024-2032) (\$MN)

Table 45 Global Blockchain in Cybersecurity Market Outlook, By IT & Telecommunication (2024-2032) (\$MN)

Table 46 Global Blockchain in Cybersecurity Market Outlook, By Healthcare & Life Sciences (2024-2032) (\$MN)

Table 47 Global Blockchain in Cybersecurity Market Outlook, By Government & Public Sector (2024-2032) (\$MN)

Table 48 Global Blockchain in Cybersecurity Market Outlook, By Retail & E-commerce (2024-2032) (\$MN)

Table 49 Global Blockchain in Cybersecurity Market Outlook, By Manufacturing (2024-2032) (\$MN)

Table 50 Global Blockchain in Cybersecurity Market Outlook, By Transportation & Logistics (2024-2032) (\$MN)

Table 51 Global Blockchain in Cybersecurity Market Outlook, By Other End Users (2024-2032) (\$MN)

Note: Tables for North America, Europe, APAC, South America, and Middle East & Africa Regions are also represented in the same manner as above.

I would like to order

Product name: Blockchain in Cybersecurity Market Forecasts to 2032 – Global Analysis By Component (Software Solutions and Services), Security Type (Private Blockchain, Public Blockchain and Hybrid Blockchain), Platform, Organization Size, Deployment Mode, Application, End User and By Geography

Product link: <https://marketpublishers.com/r/BE197F86A3E0EN.html>

Price: US\$ 4,150.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:

info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page <https://marketpublishers.com/r/BE197F86A3E0EN.html>