WALLETS, HOSPITALS AND THE CHINESE MILITARY: 19 EXAMPLES OF BLOCKCHAIN CYBERSECURITY AT WORK

July 12, 2019
Updated: October 22, 2019

Written by Sam Daley

Our money is transferred instantly via virtual bank accounts, our informational sources are vast and thorough and even online orders are delivered the next day. The amazing expediency of the digital age comes with a cost, however. Namely, our privacy.

Our dozens of accounts spread throughout the web and protected only by often weak passwords include bank accounts, health records, birthdays, social security numbers and passport information.

The information age explosion of online data has brought with it lapses in security protocols that regularly expose our most sensitive information to malicious actors. Finding a reliable cybersecurity protocol, therefore, is more important than ever before.

Industries across the board are latching onto new technology that promises to improve online security, including blockchain.

BLOCKCHAIN: A NEW WEAPON IN CYBERSECURITY

Cybercrime is such a vast and burgeoning underworld industry that it prompted Ginni Rometty, Chairman, President and CEO of IBM, to declare that "cybercrime, by definition, is the greatest threat to every profession, every industry, every company in the world."

Both dangerous and costly, cybercrime costs individuals and businesses an estimated $500 billion a year. Our current security protocols simply cannot keep up with the relentless and clever attacks, especially when they're seemingly so simple (i.e., a phishing email to a credentialed employee can expose the data of millions).

Blockchain, a Distributed Ledger Technology (DLT), is focused on creating trust in an untrusting ecosystem, making it a potentially strong cybersecurity technology.

The ledger system is decentralized, but information is transparently available to members of the specific blockchain. All members (or

BLOCKCHAIN CYBERSECURITY USES

Blockchain's inherently decentralized nature makes it the perfect technology for cybersecurity. The ledger technology has virtually endless uses in everything from medical and financial data sharing to anti-money laundering monitoring and encrypted messaging platforms.

This process creates trust while also maintaining a high level of data integrity. In essence, the distributed nature of blockchain provides no "hackable" entrance or point of failure that detrimentally exposes entire datasets.

For a deeper dive into blockchain, check out our in-depth resources here.

The cybersecurity industry can benefit from blockchain's unique features, which create a virtually impenetrable wall between a hacker and your information.

The transparent ledger allows for password-free entry.
Using biometrics, including retina scans and fingerprints, the ledger can create a single-source, uncrackable form of entry into any private data.

Decentralized storage ensures that each block contains only a small informational piece to a much larger puzzle, limiting hackable data to almost nothing.

Finally, blockchain's public record keeping system gives each node an insight into any data manipulation, exposing potential cyber crime attempts in real-time.

Blockchain in cybersecurity is widespread, and we've rounded up six industries that use it as a new weapon in the fight to protect our most

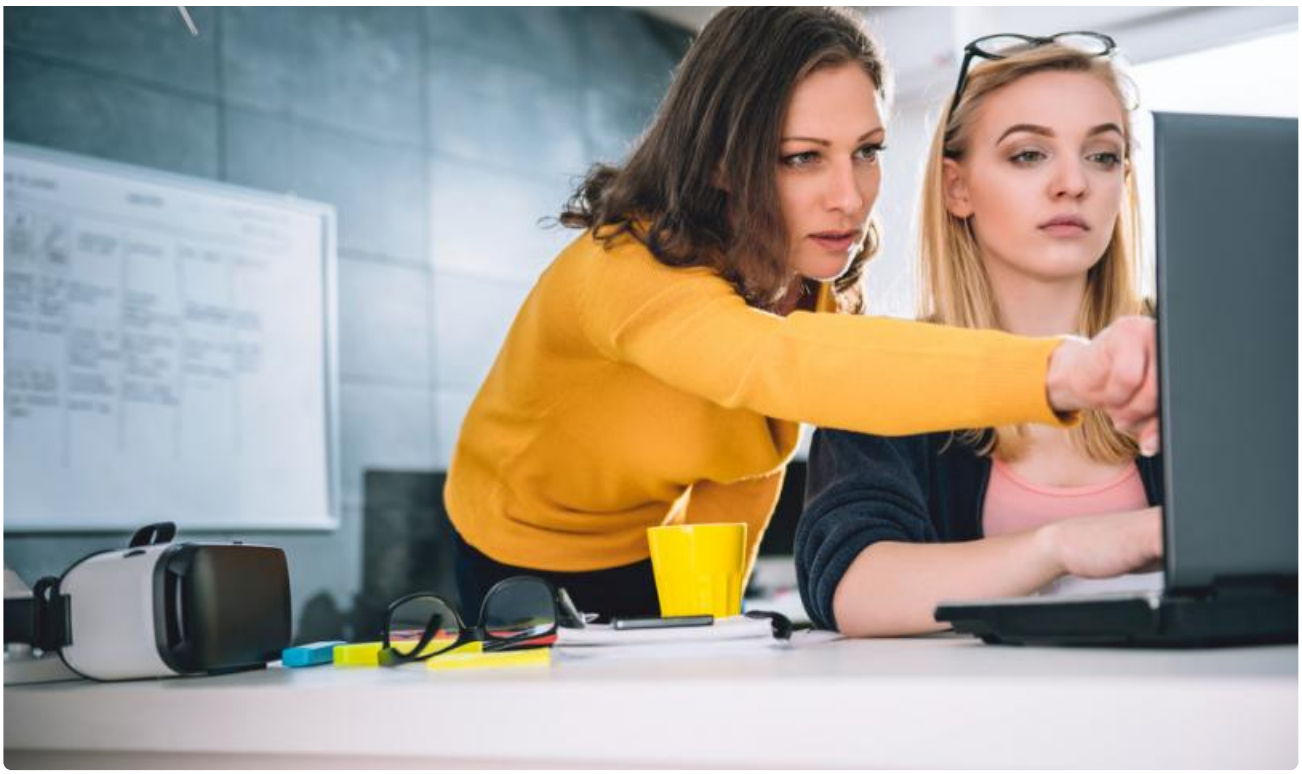
CRYPTOCURRENCIES

First implemented as the operational network behind Bitcoin, blockchain is now used in more than 1,000 different cryptocurrencies, a number that grows almost daily.

DLT protects the integrity of cryptos through encryption methods and public information sharing.

The legitimacy of cryptocurrency purchases by individuals is ensured because they can trace the transfer of the currency to its origin. Encryption helps control the amount of cryptocurrencies being created, thus stabilizing value.

These four companies use blockchain as a cybersecurity protocol in cryptocurrency trading.



MobileCoin

MOBILECOIN

Location: San Francisco, California

How it's using blockchain in cybersecurity: MobileCoin is developing an easy-to-use cryptocurrency for resource-constrained businesses who aren't currently equipped to securely handle ledger information.

The company's crypto replaces third-party transaction vendors, and it keeps all transactional data between two peers encrypted. The boosted level of security helps companies keep transparent records in a public sphere.

Industry impact: MobileCoin is designing their product to be easily integrated with WhatsApp, Facebook Messenger and Signal.

JAvvy

JAVVY

Location: Atlanta, Georgia

How it's using blockchain in cybersecurity: Javvy built a universal "wallet" that stores and trades cryptocurrencies and tokens.

The company's blockchain-based app is fully decentralized, biometric login-enabled and uses AI to detect fraudulent activity. Javvy's app helps users manage their growing crypto stashes in a more secure way.

Industry impact: Javvy's token sale will launch on November 1, 2018, and the funds will be used to expand their current crypto wallet technology.

Coinbase

COINBASE

Location: San Francisco, California

How it's using blockchain in cybersecurity: Coinbase is an exchange for users to buy and sell digital currency. Users can trade everything from Bitcoin to Litecoin to Ethereum on the company's secure blockchain platform.

Coinbase runs entirely on encryption. The company stores wallets and passwords in a secure database and requires employees to undergo a rigorous background check, all to ensure that your crypto is safe.

Founders Bank

FOUNDERS BANK

Location: Valletta, Malta

How it's using blockchain in cybersecurity: Founders Bank aims to be the world's first decentralized bank. Instead of being owned by a central authority, the bank will be owned by purchasers of its token-based equity.

The company will employ decentralized storage methods, an extensive public ledger system and encryption methods to make sure cryptocurrencies are traded and stored securely.

Industry impact: Once the bank receives its licensing, it will become the first financial institution that runs on blockchain and is owned by the public rather than by a corporation.

TRADITIONAL BANKING

Wall Street has begun to take notice of blockchain's bolstered security protocols. Traditionally known as slow movers in adopting new technologies, some of Wall Street's largest financial institutions (including JP Morgan and Bank of America) are trying to stay ahead of the curve. JP Morgan Chairman and CEO Jamie Dimon recently said the bank has been looking at blockchain for solutions to cybersecurity issues.

Trillions of dollars in cash flow combined with outdated and centralized cybersecurity protocols make the largest banks constant targets of hacking and fraud. In fact, most multinational banks currently experience cyber attacks daily and at least 85 serious infiltrations a year, with cyber criminals focused on operational risks. In its annual report, the US Office of the Comptroller of the Currency (OCC) said more sophisticated phishing attacks target employees who have access to credentialed information. The report suggests a multi-layered security protocol to decentralize risk — exactly what blockchain can provide. Here are three early adopters among "traditional" Wall Street

Santander

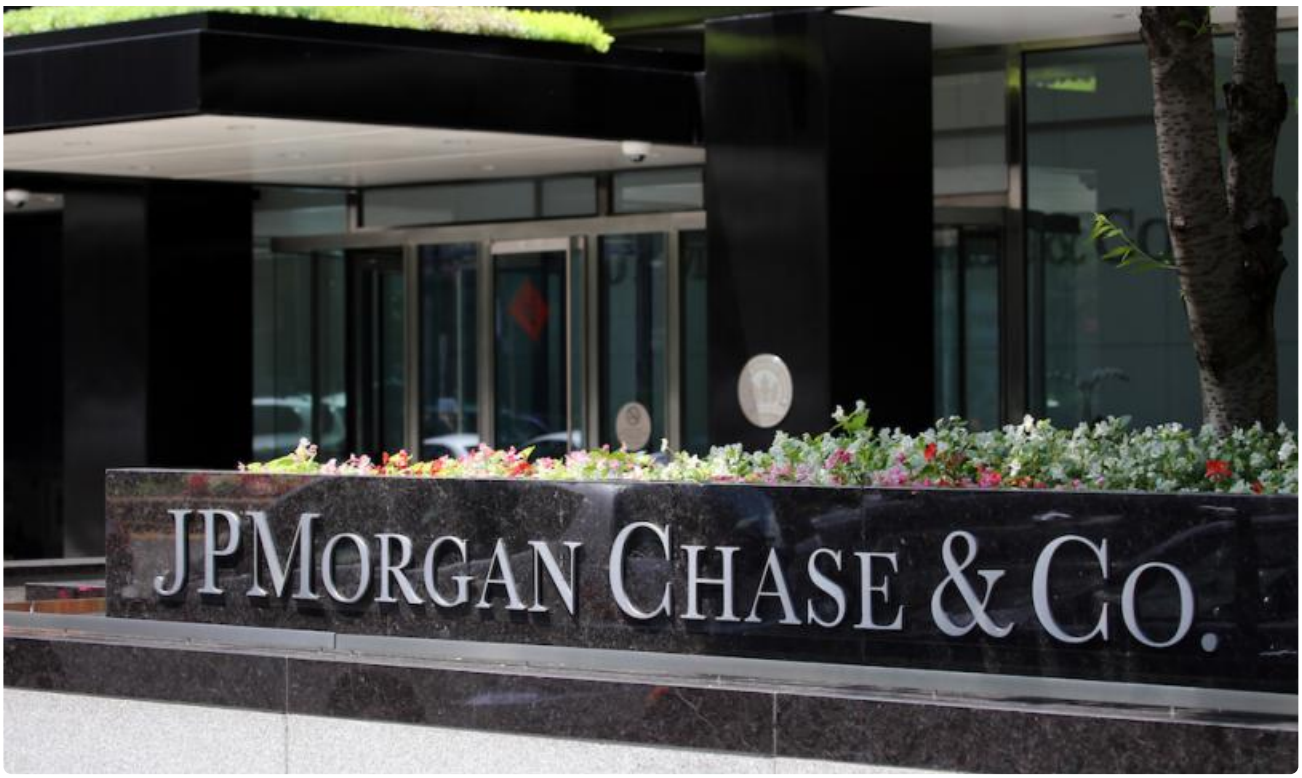
SANTANDER

Location: Boston, Massachusetts

How it's using blockchain in cybersecurity: Santander was the first bank in the UK to adopt blockchain to securitize their international payments service. It is one of the largest banks in the US with over $1.74 trillion in assets.

The bank's blockchain enables customers to securely pay between Santander accounts in Europe and South America. In partnership with Ripple, Santander's "One Pay FX" is now live in Spain, the UK, Poland and Brazil.

Industry impact: The bank is piloting a blockchain-based shareholder voting mechanism through which decentralized votes are incorruptible and in real time.



J.P. Morgan

J.P. MORGAN

Location: New York, NY

How it's using blockchain in cybersecurity: J.P. Morgan, the largest financial institution in the U.S., has developed a enterprise-focused version of Ethereum called Quorum.

The platform uses blockchain technology to process private transactions. The bank uses smart contracts on the Quorum network to implement transparent yet cryptographically-assured transactions.

Industry impact: J.P. Morgan recently provided a $150 million one-year debt issuance to the National Bank of Canada. The blockchain-dependent trial was meant to incorporate all aspects of the debt lifecycle, including origination, execution and settlement.

Barclays

BARCLAYS

Location: London, England

How it's using blockchain in cybersecurity: Barclays recently filed a patent that would use blockchain technology to bolster security in fund transfers. The Wall Street bank is possibly looking to boost the popularity and stability of cryptocurrency transfers, while using DLT to process these transfers.

Industry impact: Along with its blockchain fund transfer patent, Barclays has a patent for know-your-customer processes that enables the bank to store all personal identifying customer information on a secure blockchain.

HEALTHCARE

Like banking, the healthcare industry endures a constant barrage of cyber attacks. In fact, healthcare experiences twice the amount of phishing emails and malware attacks of any other industry. New challenges arise constantly and now include cyber attacks on IoT devices that are disguised using encrypted malware.

Not only do healthcare companies, hospitals, doctors and clinics store patient banking information, they also possess important health records. Patient data is important to cybercriminals because it demands much more money on the black market — about $50 per record. Credit card information is constantly stolen, but modern technology typically resolves any damage quickly. Exposing the social security numbers, full names, weights, heights, prescriptions and medical conditions of millions of patients can be detrimental. By threatening to release confidential information, hackers have already extorted millions of dollars from hospitals all over the world and will continue to do so unless new technologies are implemented.

allows only certain individuals to have small amounts of information that, if combined, would comprise a patient's entire health chart. The distribution of only certain information to credentialed healthcare professionals ensures that cybercriminals cannot access all identifiable aspects of an individual's health record.

Read about four healthcare companies that use blockchain cybersecurity measures to thwart attacks.

Hashed Health

HASHED HEALTH

Location: Nashville, Tennessee

How it's using blockchain in cybersecurity: Hashed Health is a healthcare innovation firm dedicated to helping the industry implement blockchain technologies. Consisting of Hashed Collective, Hashed

community. The company is also experimenting with different ledger technologies.

Hashed Health has worked with dozens of healthcare companies and hospitals to build secure digital blockchain networks for patient information sharing and internal communication channels.

Industry impact: Hashed Health convened a value-based care working group comprised of Hashed Collective members to improve quality measures and payment efficiency for hospitals and healthcare systems across the U.S.

Philips Healthcare

PHILIPS HEALTHCARE

Location: Andover, Massachusettes

healthcare ecosystem.

In partnership with hospitals all over the world, the company uses AI to discover and analyze all aspects of the healthcare system, including operational, administrative and medical data. It then implements blockchain to secure the massive amounts of data collected.

Industry impact: Philips' HealthSuite Insights platform gives healthcare systems an inside look at key pain points in the current health system, and offers AI and blockchain solutions to help fix those problems.

Health Linkages

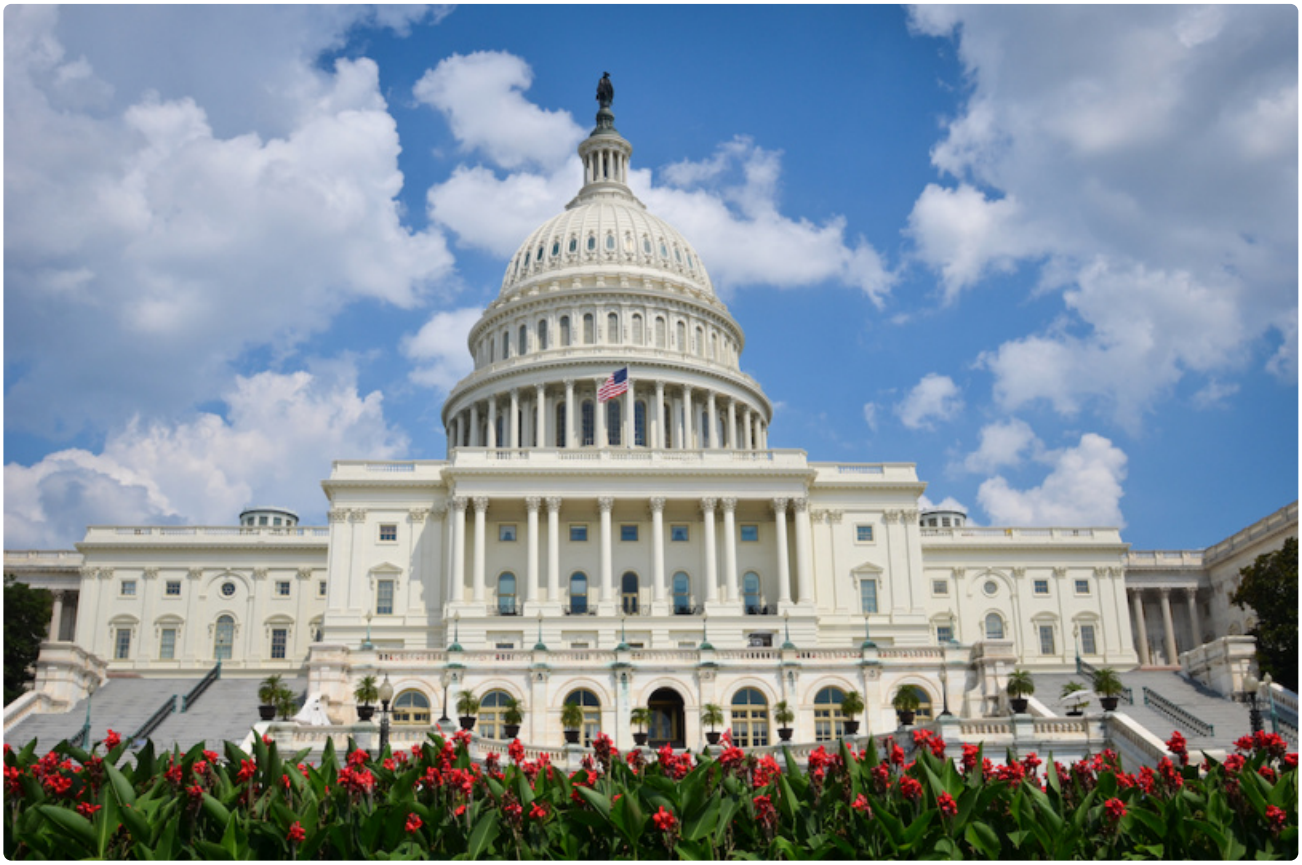
HEALTH LINKAGES

Location: Mountain View, California

How it's using blockchain in cybersecurity: Health Linkages uses blockchain to enable transparent data governance, further auditable

The company's blockchain enables only credentialed actors to share patient data, and it also maintains a chronological series of individual healthcare events, making healthcare decisions clearer for doctors.

Industry impact: Health Linkages is currently developing blockchain-based tools that show a chain-of-information so medical professionals can view a patient's history in a chronological and secure way.

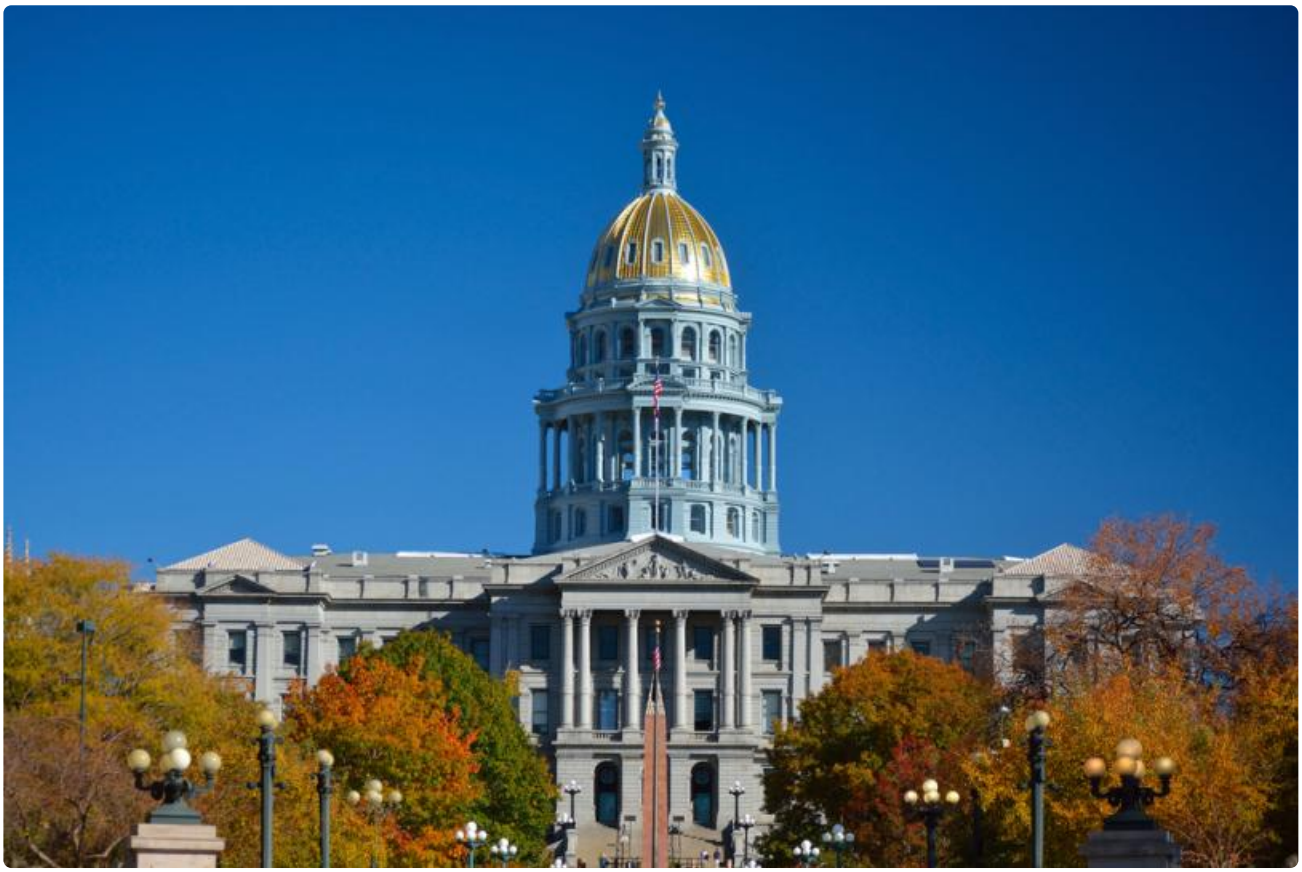


GOVERNMENT

The Office of Management and Budget (OMB) recently published a damning report on U.S. Government cybersecurity infrastructure, where phrases like "do not have the resources to combat the current threat environment" and "agencies lack visibility into what is occurring on their networks" are only the beginning. This report goes on to claim that:

methods or attacker identified
- Only 27% of agencies have the ability to detect large data compromises
- 84% of all government agencies fail at meeting basic encryption goals

These startling statistics, especially the last, can be improved with blockchain. The entire system runs on safe encryption of information, essentially putting a barrier between hackers and identifiable information. Encrypted data, decentralized information storage and publicly-visible ledgers can instill a new set of government cybersecurity priorities. Agencies would be able to quickly identify potential hacks and trace the manipulated data to its origin. These governments and agencies, in attempting to be among the first governmental blockchain adapters, are pioneering ways to implement DLT into everyday cybersecurity protocol.



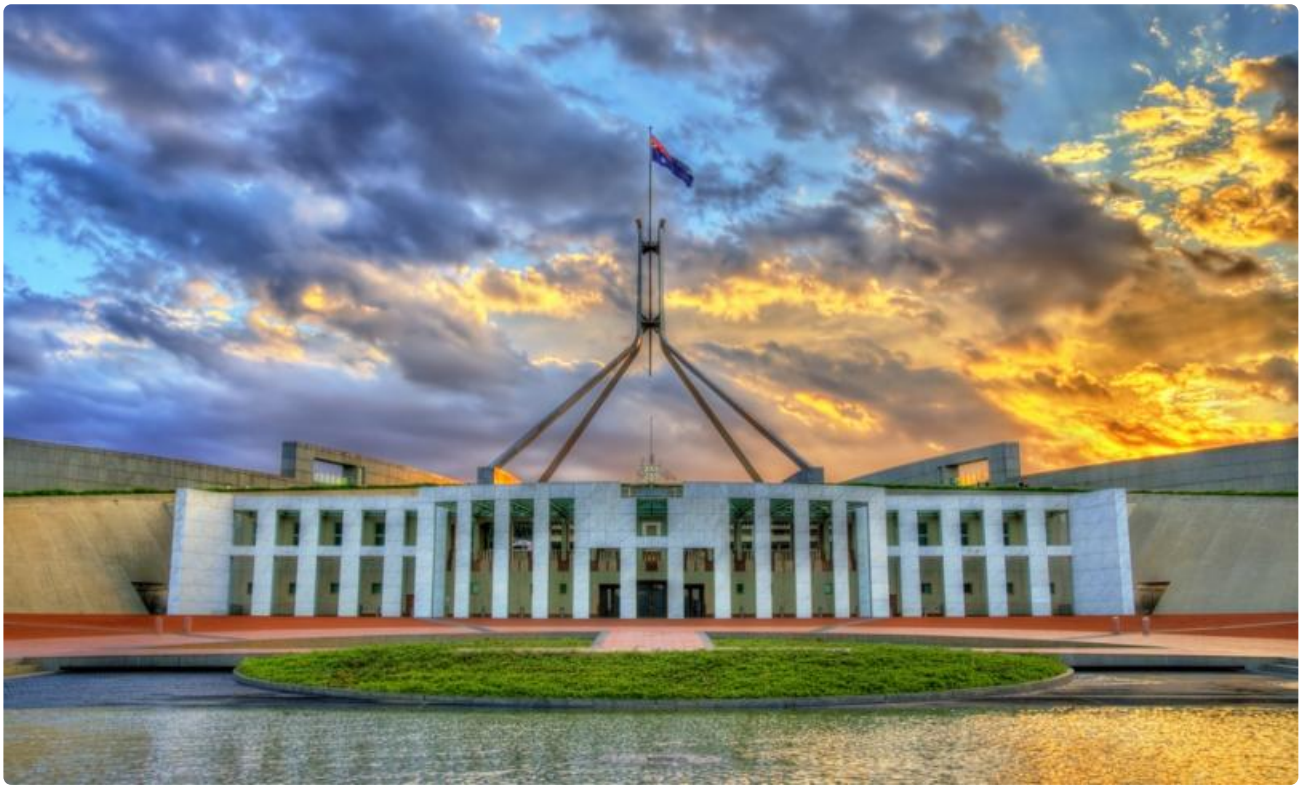
The State of Colorado

Location: Denver, Colorado

How it's using blockchain in cybersecurity: The Colorado Senate passed a bill in May 2018 that implores the government to consider blockchain for data protection and the secure storage of records.

Colorado reportedly experiences six to eight million attempted attacks each day, giving the state every reason to implement blockchain's encryption methods to protect its most vital networks.

Industry impact: As it expands the blockchain cybersecurity protocols past their infancy stages, the Colorado State Congress is looking to pass more bills involving the uniform definition of a "token." In the meantime, check out five Colorado-based blockchain companies that are making a big impact.



Australia

AUSTRALIA

Location: Canberra, Australia

The country recently prioritized the development of a cybersecurity network that runs on DLT.

The country's network is now in the early stages of implementation, but government officials see it blossoming into a valuable asset.

Industry impact: Australia recently partnered with IBM to create a governmental blockchain ecosystem for securely storing government documents. The country's federal government hopes this will be seen as a model for other governments going forward.

Malta

MALTA

Location: Valletta, Malta

How it's using blockchain in cybersecurity: Malta is quickly embracing blockchain in its bid to become "#BlockchainIsland."

The small nation is currently implementing blockchain cybersecurity measures in its finance sector, and the government is looking into how the ledger technology could be useful in safeguarding government documents and sensitive citizen information.

Industry impact: The Government of Malta has been very welcoming to companies looking to headquarter and ICO in the island nation. Malta's Digital Innovation Authority was recently created to help boost innovation and investment in the island's burgeoning tech scene.

DEFENSE AND MILITARY

military pioneered the Internet to share important detailed information with dispersed groups all over the world, and it created GPS to better grasp military positioning. Will blockchain be the next breakthrough technology that's promoted by the defense sector?

According to Accenture, 86% of defense companies plan to integrate blockchain in the protocols within the next three years, especially in cybersecurity. Blockchain is seen as a legitimate data safeguard for militaries, defense contractors and aerospace companies that house some of the most sensitive information (coordinates for missions, identifiable employee/personnel information, new technologies, etc.).

These militaries and defense companies use blockchain's encryption and decentralization methods to improve data security and maximize privacy.

DARPA

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)

Location: Arlington County, Virginia

How it's using blockchain in cybersecurity: The Defense Advanced Research Projects Agency (DARPA) is the technology development branch of the U.S. Army and is looking into blockchain mainly for its usefulness in encryption and secure data transfer.

Industry impact: Engineers are creating an encrypted, blockchain-based messaging system for U.S. military personnel to instantaneously share vital information to any location on the globe without worrying about foreign hackers listening in.

CHINESE MILITARY

Location: Beijing, China

How it's using blockchain in cybersecurity: The Chinese military views blockchain as a way to improve efficiency and defend against foreign adversaries that attempt to tamper with or delete vital government and military information.

Industry impact: Although they have been less-than-specific about certain projects, China's government and military are known to be looking into blockchain cybersecurity to protect everything from intelligence operation information to communication between officials.

Lockheed Martin

LOCKHEED MARTIN

Location: Bethesda, Maryland

How it's using blockchain in cybersecurity: Lockheed Martin is the first U.S. defense contractor to implement blockchain into its protocol.

The company is teaming up with Guardtime Federal to implement blockchain cybersecurity protocol measures in the engineering systems, supply chain risk management and software development.

Industry impact: Lockheed Martin is in the early stages of researching the use of blockchain to protect every step of its weapon development systems and ensure that vital and dangerous weaponry is incorruptible.

INTERNET OF THINGS (IOT)

products can be found in almost every aspect of our lives. From robo-sprinklers to bluetooth-enabled bike locks to smart kitchen appliances, everything is wirelessly connected.

There have been thousands of reported IoT device hacks over the last few years, a number that will surely increase in light of estimates that there will be 75 billion connected devices by 2025. One cybersecurity-related report found that hackers were able to bypass the security measures in an implantable cardiac device, which gave them the ability to deplete the battery as well as administer incorrect heart shocks. Additionally, it was reported that hackers targeted the camera of a "smart" baby monitor by obtaining a simple IP address. The hackers had full control of the machine to watch through the camera and listen in on conversations.

As the IoT device market continues to grow, so too does the need for an enhanced form of cybersecurity. Blockchain provides a safe infrastructure for the transfer of data from one device to another without the interference of malicious actors. Decentralized control enables IoT devices to create audit trails and tracking methods for registering and using products.

These three companies are focusing on diminishing hacking opportunities and maximizing cybersecurity strength within the Internet of Things.

Hdac

HDAC

Location: Zug, Switzerland

How it's using blockchain in cybersecurity: Hdac's blockchain platform for IoT devices supports everything from payments between devices to

network.

Industry impact: Already successful with smart wallets, Hdac is now focusing on introducing blockchain IoT cybersecurity protocols to all connected devices in smart factories, smart homes and smart buildings.

Cisco

CISCO

Location: San Jose, California

How it's using blockchain in cybersecurity: As part of the Trusted IoT Alliance, networking giant Cisco belongs to a group that is considering scaling technologies to enhance the security of IoT products. The company believes blockchain pairs well with IoT devices because the ledger technology eliminates single points of failure and secures data through encryption.

Industry impact: Cisco has already worked with supply chain company Flex and hardware company Rockwell Automation to establish blockchain networks in the companies' shipping and manufacturing processes.

Filament

FILAMENT

Location: Reno, Nevada

How it's using blockchain in cybersecurity: Filament creates blockchain-enabled software and hardware to ensure the data integrity

The software is a smart contract system that helps supply chain management teams manage cryptographic chain-of-custody by which teams can safely track and manage logistical information.

Industry impact: Filament's Blocklet USB unleashes several different blockchain communication tracing and protection tools at one time, and it is as-easy to install as inserting a USB.

Blockchain Cybersecurity